ID: 634965
Sample Name: View Shared File.pdf
Cookbook: defaultwindowspdfcookbook.jbs
Time: 07:38:13
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

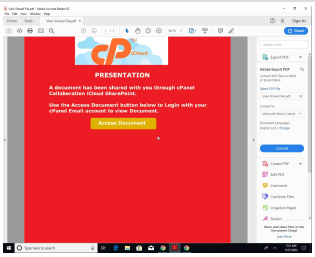
Windows Analysis Report

View Shared File.pdf

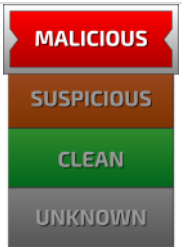
Overview

General Information

Sample Name:	View Shared File.pdf
Analysis ID:	634965
MD5:	0a2fecc6ab069d…
SHA1:	7f1092ab0289b7..
SHA256:	4fab88614d6668..
Infos:	



Detection



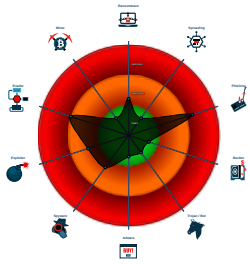
HTMLPhisher

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- Antivirus detection for URL or domain
- Contains functionality to check if a d…
- Uses code obfuscation techniques (…
- Found evasive API chain (date chec…
- No HTML title found
- Detected potential crypto function
- Contains functionality to create guar…
- Contains functionality to query CPU…
- Found potential string decryption / a…
- Sample execution stops while proce…
- Contains functionality to check if a d…

Classification



Process Tree

- **System is w10x64**
- AcroRd32.exe (PID: 4592 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Desktop\View Shared File.pdf MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 5236 cmdline: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" --type=renderer /prefetch:1 "C:\Users\user\Desktop\View Shared File.pdf MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 6240 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6416 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1692,9505094711010095436,2813685380730867450,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=4522651327695846108 --lang=en-US --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=4522651327695846108 --renderer-client-id=2 --mojo-platform-channel-handle=1704 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6436 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=gpu-process --field-trial-handle=1692,9505094711010095436,2813685380730867450,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --lang=en-US --gpu-preferences=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --service-request-channel-token=10689791772710628581 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job --ignored=" --type=renderer " / prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6476 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1692,9505094711010095436,2813685380730867450,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=1168505979000462944 --lang=en-US --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=1168505979000462944 --renderer-client-id=4 --mojo-platform-channel-handle=1812 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
      - conhost.exe (PID: 5200 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - RdrCEF.exe (PID: 6588 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1692,9505094711010095436,2813685380730867450,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=12017203034287935800 --lang=en-US --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=12017203034287935800 --renderer-client-id=5 --mojo-platform-channel-handle=2192 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6168 cmdline: "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1692,9505094711010095436,2813685380730867450,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=1325300201368898226 --lang=en-US --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=1325300201368898226 --renderer-client-id=6 --mojo-platform-channel-handle=2804 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
  - chrome.exe (PID: 3152 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation -- "http://v2.bpkbsaya.com/wp-includes/css/cPanel.SharePoint_documentOnline/redirecting.php MD5: C139654B5C1438A95B321BB01AD63EF6)

- chrome.exe (PID: 7016 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1556,1458980921024501746,2057635213361371639,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1908 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- elevation_service.exe (PID: 3876 cmdline: C:\Program Files\Google\Chrome\Application\85.0.4183.121\elevation_service.exe MD5: AFD137B53BA091ACBA569255B16DF837)
- ChromeRecovery.exe (PID: 6240 cmdline: "C:\Program Files\Google\Chrome\ChromeRecovery\scoped_dir3876_980132676\ChromeRecovery.exe" --appguid={8A69D345-D564-463c-AFF1-A69D9E530F96} --browser-version=85.0.4183.121 --sessionid={3300d716-561c-4453-9d4f-82432db65734} --system MD5: 49AC3C96D270702A27B4895E4CE1F42A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
62445.1.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
38924.3.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
96408.4.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
57468.5.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
75415.6.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Click to see the 3 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

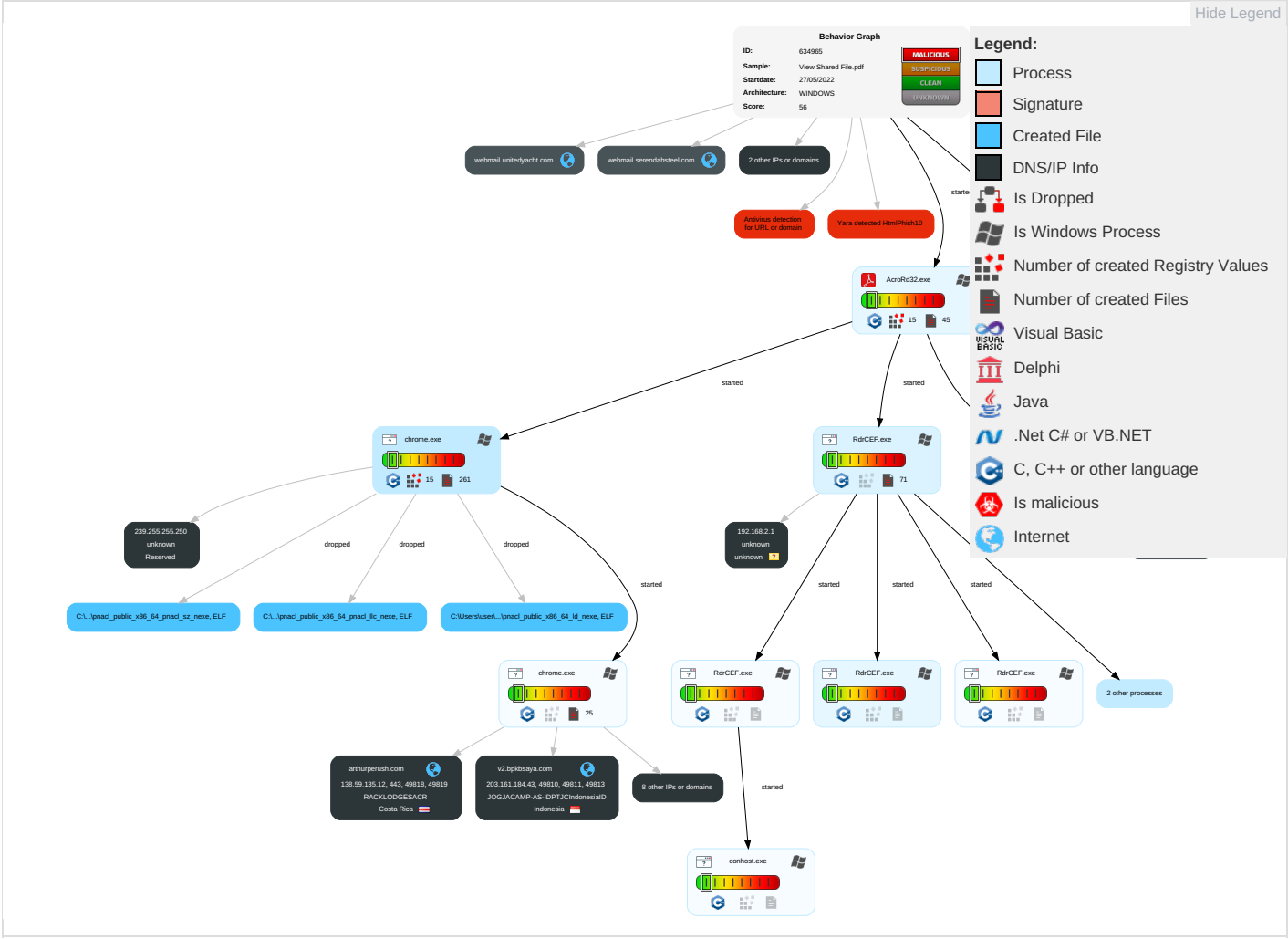
Phishing

Yara detected HtmlPhish10

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	3 Native API	Path Interception	2 Process Injection	3 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	3 Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	3 1 Security Software Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Process Injection	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	5 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Obfuscated Files or Information	LSA Secrets	1 4 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

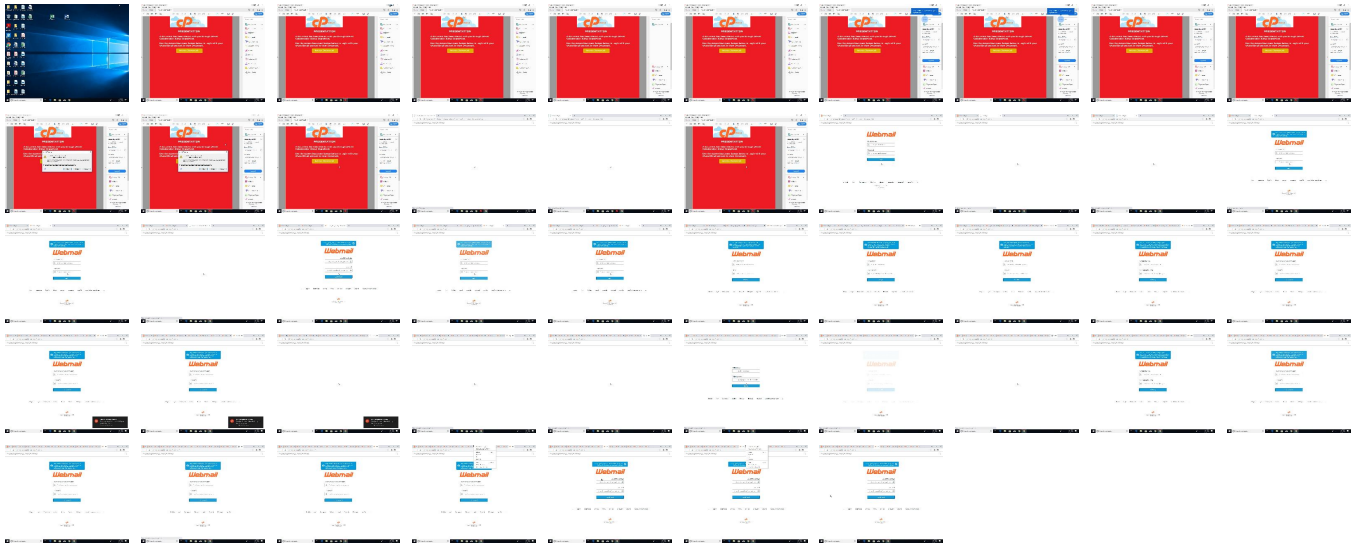
Behavior Graph

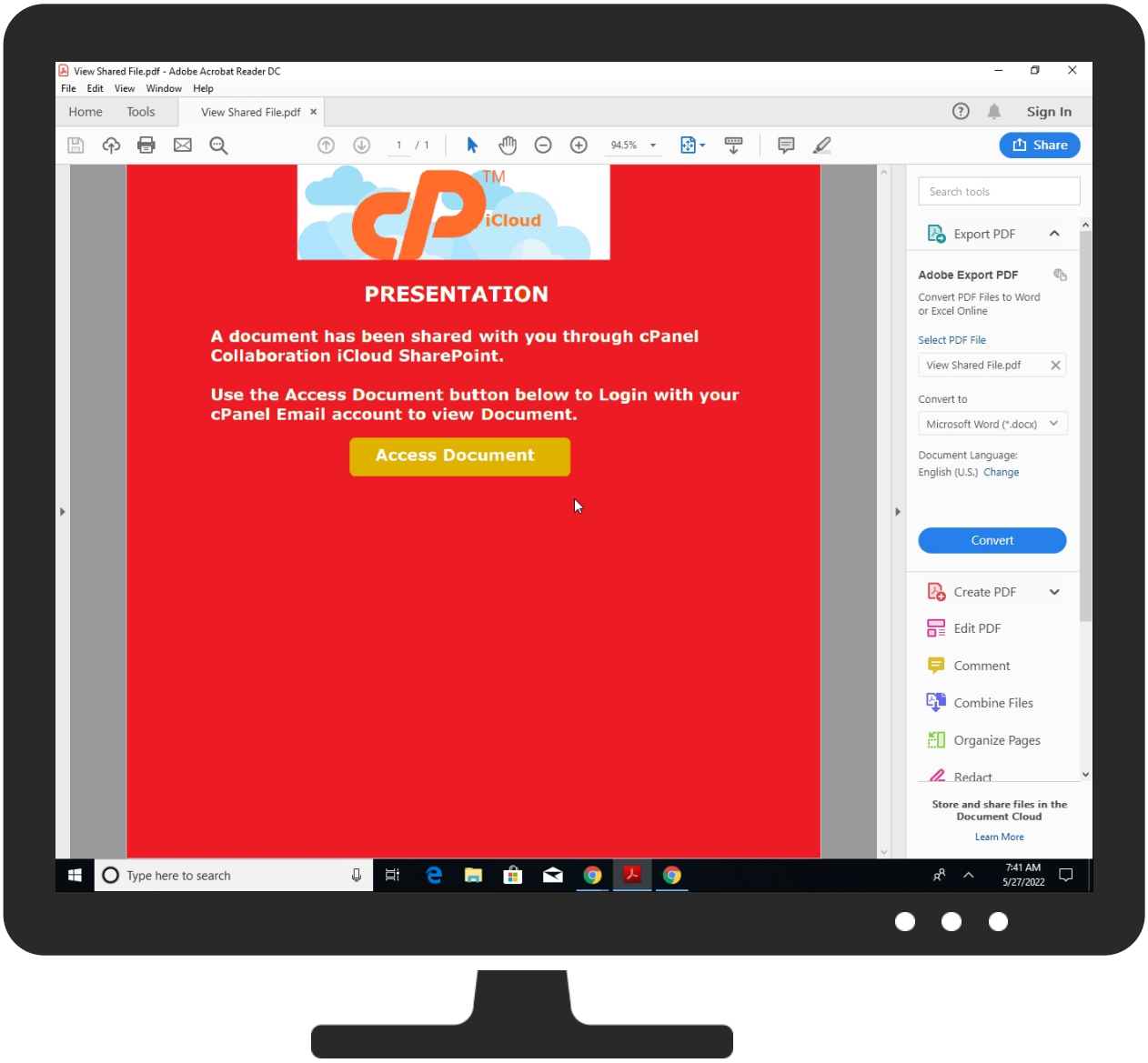


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
View Shared File.pdf	0%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files\Google\Chrome\ChromeRecovery\scoped_dir3876_980132676\ChromeRecovery.exe	0%	Metadefender		Browse
C:\Program Files\Google\Chrome\ChromeRecovery\scoped_dir3876_980132676\ChromeRecovery.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\3152_1449025593_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\3152_1449025593_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\3152_1449025593_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\3152_1449025593_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\3152_1449025593_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\3152_1449025593_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
bpkbsaya.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://arthurperush.com/css/cPanel.SharePoint_documentOnline/login.html	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1463518546/unprotected/cpanel/images/notice-success.png	0%	Avira URL Cloud	safe	
http://https://arthurperush.com/css/cPanel.SharePoint_documentOnline/login.html2	0%	Avira URL Cloud	safe	
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1463518546/unprotected/cpanel/images/warning.png	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/iew	0%	Avira URL Cloud	safe	
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Regular-webfont.woff	0%	Avira URL Cloud	safe	
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Bold-webfont.woff	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Regular-webfont.ttf	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/U	0%	Avira URL Cloud	safe	
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1508464910/unprotected/cpanel/style_v2_optimized.css	0%	Avira URL Cloud	safe	
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Regular-webfont.woff	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	0%	Avira URL Cloud	safe	
http://www.pdf-tools.com)	0%	Avira URL Cloud	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/w	0%	Avira URL Cloud	safe	
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Semibold-webfont.woff	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://api.echosign.comA	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/rsi	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/)	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1463518546/unprotected/cpanel/images/notice-info.png	0%	Avira URL Cloud	safe	
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/open_sans.min.css	0%	Avira URL Cloud	safe	
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Bold-webfont.woff	0%	Avira URL Cloud	safe	
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1463518546/unprotected/cpanel/images/notice-error.png	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/6	0%	Avira URL Cloud	safe	
http://v2.bpkbsaya.com/wp-includes/css/cPanel.SharePoint_documentOnline/redirecting.php2	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/1.0/	0%	URL Reputation	safe	
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1386192030/unprotected/cpanel/fonts/open_sans/open_sans.min.css	0%	Avira URL Cloud	safe	
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1547665285/unprotected/cpanel/images/icon-password.png	0%	Avira URL Cloud	safe	
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Semibold-webfont.ttf	0%	Avira URL Cloud	safe	
http://v2.bpkbsaya.com/wp-includes/css/cPanel.SharePoint_documentOnline/redirecting.php	0%	Avira URL Cloud	safe	
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1463518546/unprotected/cpanel/images/icon-password.png	0%	Avira URL Cloud	safe	
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1547665285/unprotected/cpanel/images/icon-username.png	0%	Avira URL Cloud	safe	
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Bold-webfont.ttf	0%	Avira URL Cloud	safe	
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1463518546/unprotected/cpanel/images/icon-username.png	0%	Avira URL Cloud	safe	
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1463518546/unprotected/cpanel/images/webmail-logo.svg	0%	Avira URL Cloud	safe	
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1458739301/unprotected/cpanel/images/webmail-logo.svg	0%	Avira URL Cloud	safe	
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Semibold-webfont.woff	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	0%	Avira URL Cloud	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/ut	0%	Avira URL Cloud	safe	
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1630269605/unprotected/cpanel/style_v2_optimized.css	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
webmail.serendahsteel.com	103.6.196.136	true	false		unknown
bpkbsaya.com	203.161.184.43	true	false	• 0%, Virustotal, Browse	unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.203.109	true	false		high
arthurperush.com	138.59.135.12	true	false		unknown
clients.l.google.com	216.58.215.238	true	false		high
v2.bpkbsaya.com	203.161.184.43	true	false		unknown
webmail.unitedyacht.com	72.9.144.117	true	false		unknown
ipv4.imgur.map.fastly.net	151.101.112.193	true	false		unknown
clients2.google.com	unknown	unknown	false		high
i.imgur.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1463518546/unprotected/cpanel/images/notice-success.png	false	• Avira URL Cloud: safe	unknown
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1463518546/unprotected/cpanel/images/warning.png	false	• Avira URL Cloud: safe	unknown
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Regular-webfont.woff	false	• Avira URL Cloud: safe	unknown
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Bold-webfont.woff	false	• Avira URL Cloud: safe	unknown
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Regular-webfont.ttf	false	• Avira URL Cloud: safe	unknown
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1508464910/unprotected/cpanel/style_v2_optimized.css	false	• Avira URL Cloud: safe	unknown
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Regular-webfont.woff	false	• Avira URL Cloud: safe	unknown
http://https://arthurperush.com/css/cPanel.SharePoint_documentOnline/login.html	true	• SlashNext: Credential Stealing type: Phishing & Social Engineering	unknown
http://https://arthurperush.com/css/cPanel.SharePoint_documentOnline/login.html	true	• SlashNext: Credential Stealing type: Phishing & Social Engineering	unknown
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Semibold-webfont.woff	false	• Avira URL Cloud: safe	unknown
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1463518546/unprotected/cpanel/images/notice-info.png	false	• Avira URL Cloud: safe	unknown
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/open_sans.min.css	false	• Avira URL Cloud: safe	unknown
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Bold-webfont.woff	false	• Avira URL Cloud: safe	unknown
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1463518546/unprotected/cpanel/images/notice-error.png	false	• Avira URL Cloud: safe	unknown
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://i.imgur.com/VCmmJUv.png	false		high
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1386192030/unprotected/cpanel/fonts/open_sans/open_sans.min.css	false	• Avira URL Cloud: safe	unknown
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1547665285/unprotected/cpanel/images/icon-password.png	false	• Avira URL Cloud: safe	unknown
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Semibold-webfont.ttf	false	• Avira URL Cloud: safe	unknown
http://v2.bpkbsaya.com/wp-includes/css/cPanel.SharePoint_documentOnline/redirecting.php	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1463518546/unprotected/cpanel/images/icon-password.png	false	• Avira URL Cloud: safe	unknown
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1547665285/unprotected/cpanel/images/icon-username.png	false	• Avira URL Cloud: safe	unknown
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Bold-webfont.ttf	false	• Avira URL Cloud: safe	unknown
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1463518546/unprotected/cpanel/images/icon-username.png	false	• Avira URL Cloud: safe	unknown
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1463518546/unprotected/cpanel/images/webmail-logo.svg	false	• Avira URL Cloud: safe	unknown
http://https://webmail.unitedyacht.com/cPanel_magic_revision_1458739301/unprotected/cpanel/images/webmail-logo.svg	false	• Avira URL Cloud: safe	unknown
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Semibold-webfont.woff	false	• Avira URL Cloud: safe	unknown
http://https://webmail.serendahsteel.com/cPanel_magic_revision_1630269605/unprotected/cpanel/style_v2_optimized.css	false	• Avira URL Cloud: safe	unknown

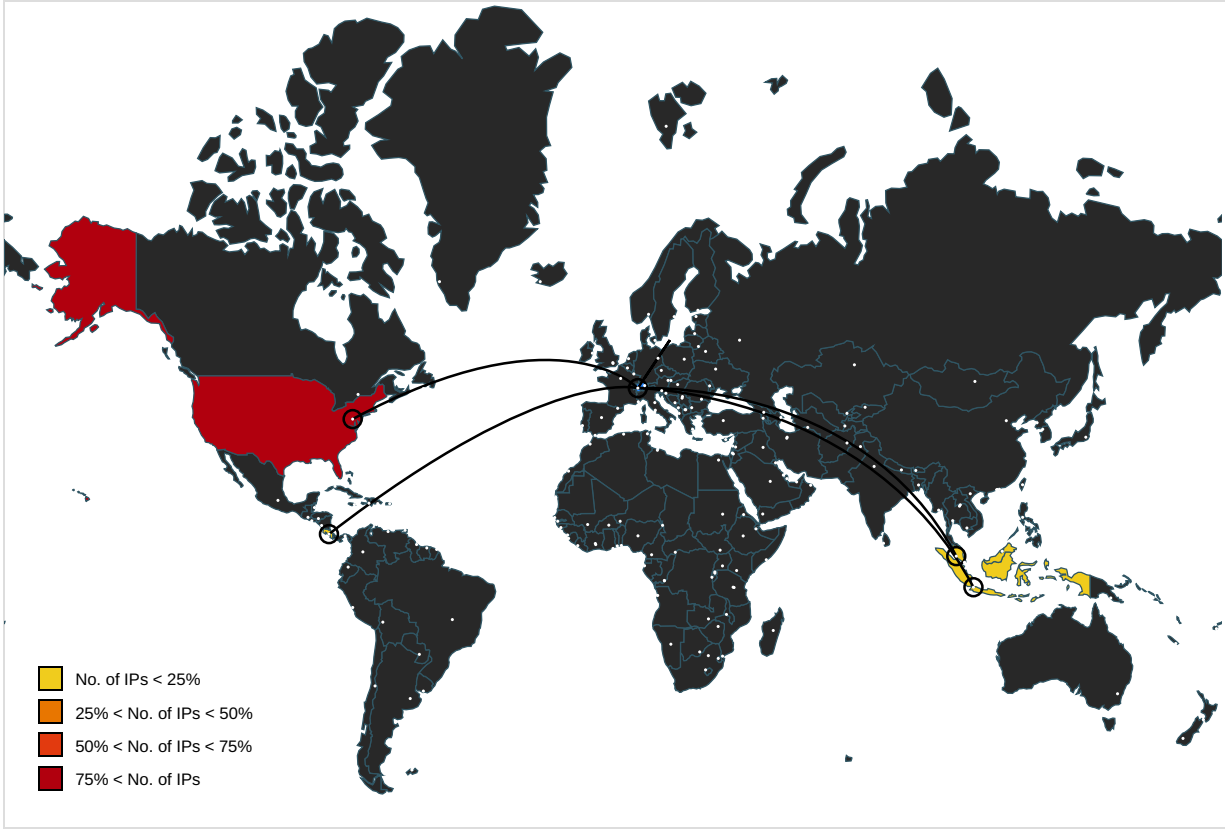
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://arthurperush.com/css/cPanel.SharePoint_documentOnline/login.html2	History Provider Cache.34.dr	true	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfe/ns/id/i	AcroRd32.exe, 00000001.00000000.41945316 0.000000000AEA0000.00000004.00000001.000 20000.00000000.sdmp, AcroRd32.exe, 00000 001.00000000.435987288.000000000AEA0000. 00000004.00000001.00020000.00000000.sdmp	false		high
http://www.aiim.org/pdfe/ns/id/l	AcroRd32.exe, 00000001.00000000.41945316 0.000000000AEA0000.00000004.00000001.000 20000.00000000.sdmp, AcroRd32.exe, 00000 001.00000000.435987288.000000000AEA0000. 00000004.00000001.00020000.00000000.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/iew	AcroRd32.exe, 00000001.00000000.43576418 6.000000000ADAB000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.google.com/images/cleardot.gif	craw_window.js.34.dr	false		high
http://https://play.google.com	dbc05ae3-04c6-437c-9d41-b2249c7cf2c0.tmp.35.dr, 489464f3-d7d6-4730-89cc-46a1e014e96b.tmp.35.dr, 9201d6f7-b73e-4a17-9370-924f601aeb69.tmp.35.dr	false		high
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000001.00000000.43571294 5.000000000AD3B000.00000004.00000001.000 20000.00000000.sdmp	false		high
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000001.00000000.41945316 0.000000000AEA0000.00000004.00000001.000 20000.00000000.sdmp, AcroRd32.exe, 00000 001.00000000.435987288.000000000AEA0000. 00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/U	AcroRd32.exe, 00000001.00000000.43586349 1.000000000AE08000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://sandbox.google.com/payments/v4/js/integrator.js	manifest.json1.34.dr, craw_window.js.34.dr	false		high
http://https://accounts.google.com/MergeSession	craw_window.js.34.dr	false		high
http://https://www.google.com	dbc05ae3-04c6-437c-9d41-b2249c7cf2c0.tmp.35.dr, 489464f3-d7d6-4730-89cc-46a1e014e96b.tmp.35.dr, 9201d6f7-b73e-4a17-9370-924f601aeb69.tmp.35.dr	false		high
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000001.00000000.43571294 5.000000000AD3B000.00000004.00000001.000 20000.00000000.sdmp	false		high
http://https://api.echosign.com	AcroRd32.exe, 00000001.00000000.41945316 0.000000000AEA0000.00000004.00000001.000 20000.00000000.sdmp, AcroRd32.exe, 00000 001.00000000.435987288.000000000AEA0000. 00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000001.00000000.43586349 1.000000000AE08000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.pdf-tools.com)	AcroRd32.exe, 00000001.00000000.41472782 4.000000000A2A2000.00000004.00000001.000 20000.00000000.sdmp, AcroRd32.exe, 00000 001.00000000.419453160.000000000AEA0000. 00000004.00000001.00020000.00000000.sdmp, AcroRd32.exe, 00000001.00000000.435987 288.000000000AEA0000.00000004.00000001.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://accounts.google.com	dbc05ae3-04c6-437c-9d41-b2249c7cf2c0.tmp.35.dr, 489464f3-d7d6-4730-89cc-46a1e014e96b.tmp.35.dr, 9201d6f7-b73e-4a17-9370-924f601aeb69.tmp.35.dr	false		high
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000001.00000000.41945316 0.000000000AEA0000.00000004.00000001.000 20000.00000000.sdmp, AcroRd32.exe, 00000 001.00000000.435987288.000000000AEA0000. 00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/w	AcroRd32.exe, 00000001.00000000.43586349 1.000000000AE08000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 00000001.00000000.43571294 5.000000000AD3B000.00000004.00000001.000 20000.00000000.sdmp	false		high
http://https://apis.google.com	dbc05ae3-04c6-437c-9d41-b2249c7cf2c0.tmp.35.dr, 489464f3-d7d6-4730-89cc-46a1e014e96b.tmp.35.dr, 9201d6f7-b73e-4a17-9370-924f601aeb69.tmp.35.dr	false		high
http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1	craw_window.js.34.dr	false		high
http://https://api.echosign.comA	AcroRd32.exe, 00000001.00000000.41945316 0.000000000AEA0000.00000004.00000001.000 20000.00000000.sdmp, AcroRd32.exe, 00000 001.00000000.435987288.000000000AEA0000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/rsi	AcroRd32.exe, 00000001.00000000.43576418 6.000000000ADAB000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www-googleapis-staging.sandbox.google.com	craw_window.js.34.dr, craw_background.js.34.dr	false		high
http://https://clients2.google.com	dbc05ae3-04c6-437c-9d41-b2249c7cf2c0.tmp.35.dr, 489464f3-d7d6-4730-89cc-46a1e014e96b.tmp.35.dr, 9201d6f7-b73e-4a17-9370-924f601aeb69.tmp.35.dr	false		high
http://www.aiim.org/pdfa/ns/property#	AcroRd32.exe, 00000001.00000000.43571294 5.000000000AD3B000.00000004.00000001.000 20000.00000000.sdmp	false		high
http://cipa.jp/exif/1.0/)	AcroRd32.exe, 00000001.00000000.41945316 0.000000000AEA0000.00000004.00000001.000 20000.00000000.sdmp, AcroRd32.exe, 00000 001.00000000.435987288.000000000AEA0000. 00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dns.google	dbc05ae3-04c6-437c-9d41-b2249c7cf2c0.tmp.35.dr, 7e1e79ea-bcff-45de-845a-43cf18598136.tmp.35.dr, 7016b328-c69b-4427-bf66-a5317616c2ba.tmp.35.dr, 489464f3-d7d6-4730-89cc-46a1e014e96b.tmp.35.dr, 9201d6f7-b73e-4a17-9370-924f601aeb69.tmp.35.dr, 19fa8736-0cad-4232-b7d2-b453200b1e8b.tmp.35.dr	false	• URL Reputation: safe	unknown
http://https://github.com/google/closure-library/wiki/goog.module:-an-ES6-module-like-alternative-to-goog.p	craw_window.js.34.dr, craw_background.js.34.dr	false		high
http://https://www.google.com/intl/en-US/chrome/blank.html	craw_background.js.34.dr	false		high
http://https://ogs.google.com	dbc05ae3-04c6-437c-9d41-b2249c7cf2c0.tmp.35.dr, 489464f3-d7d6-4730-89cc-46a1e014e96b.tmp.35.dr, 9201d6f7-b73e-4a17-9370-924f601aeb69.tmp.35.dr	false		high
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000001.00000000.43571294 5.000000000AD3B000.00000004.00000001.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 00000001.00000000.41945316 0.000000000AEA0000.00000004.00000001.000 20000.00000000.sdmp, AcroRd32.exe, 00000 001.00000000.435987288.000000000AEA0000. 00000004.00000001.00020000.00000000.sdmp	false		high
http://www.aiim.org/pdfa/ns/property#8	AcroRd32.exe, 00000001.00000000.43571294 5.000000000AD3B000.00000004.00000001.000 20000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 00000001.00000000.43571294 5.000000000AD3B000.00000004.00000001.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.npes.org/pdfx/ns/id/6	AcroRd32.exe, 00000001.00000000.41945316 0.000000000AEA0000.00000004.00000001.000 20000.00000000.sdmp, AcroRd32.exe, 00000 001.00000000.435987288.000000000AEA0000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://payments.google.com/payments/v4/js/integrator .js	manifest.json1.34.dr, craw_window.js.34.dr	false		high
http://v2.bpkbsaya.com/wp-includes/css/cPanel.SharePoint_documentOnline/redirecting.php2	History Provider Cache.34.dr	false	• Avira URL Cloud: safe	unknown
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 00000001.00000000.43571294 5.000000000AD3B000.00000004.00000001.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000001.00000000.41945316 0.000000000AEA0000.00000004.00000001.000 20000.00000000.sdmp, AcroRd32.exe, 00000 001.00000000.435987288.000000000AEA0000. 00000004.00000001.00020000.00000000.sdmp	false		high
http:// https://chromium.googlesource.com/a/native_client/pnacl-llvm.git	pnacl_public_x86_64_crtbegin_for_eh_o.34.dr	false		high
http://cipa.jp/exif/1.0/1.0/	AcroRd32.exe, 00000001.00000000.41945316 0.000000000AEA0000.00000004.00000001.000 20000.00000000.sdmp, AcroRd32.exe, 00000 001.00000000.435987288.000000000AEA0000. 00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com/images/x2.gif	craw_window.js.34.dr	false		high
http://llvm.org/):	pnacl_public_x86_64_pnacl_llc_nexe.34.dr, pnacl_public_x86_64_pnacl_sz_nexe.34.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.34.dr	false		high
http:// https://code.google.com/p/nativeclient/issues/entry%s:	pnacl_public_x86_64_ld_nexe.34.dr	false		high
http:// https://code.google.com/p/nativeclient/issues/entry	pnacl_public_x86_64_ld_nexe.34.dr	false		high
http://www.aiim.org/pdfa/ns/field#	AcroRd32.exe, 00000001.00000000.43571294 5.000000000AD3B000.00000004.00000001.000 20000.00000000.sdmp	false		high
http:// https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	AcroRd32.exe, 00000001.00000000.43576418 6.000000000ADAB000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://clients2.googleusercontent.com	dbc05ae3-04c6-437c-9d41-b2249c7cf2c0.tmp.35.dr, 489464f3-d7d6-4730-89cc-46a1e014e96b.tmp.35.dr, 9201d6f7-b73e-4a17-9370-924f601aeb69.tmp.35.dr	false		high
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000001.00000000.39820399 6.0000000008F6F000.00000004.00000001.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000001.00000000.39828918 0.000000000A290000.00000004.00000001.000 20000.00000000.sdmp	false		high
http://www.aiim.org/pdfa/ns/property#x(	AcroRd32.exe, 00000001.00000000.43571294 5.000000000AD3B000.00000004.00000001.000 20000.00000000.sdmp	false		high
http:// https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/ut	AcroRd32.exe, 00000001.00000000.43576418 6.000000000ADAB000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.google.com/	manifest.json1.34.dr	false		high
http:// https://chromium.googlesource.com/a/native_client/pnacl-clang.git	pnacl_public_x86_64_crtbegin_for_eh_o.34.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json1.34.dr, manifest.json0.34.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.161.184.43	bpkbsaya.com	Indonesia		46050	JOGJACAMP-AS-IDPTJCIndonesiaID	false
216.58.215.238	clients.l.google.com	United States		15169	GOOGLEUS	false
72.9.144.117	webmail.unitedyacht.com	United States		393398	ASN-DISUS	false
103.6.196.136	webmail.serendahsteel.com	Malaysia		46015	EXABYTES-AS-APExaBytesNetworkSdnBhdMY	false
138.59.135.12	arthurperush.com	Costa Rica		28110	RACKLODGESACR	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
151.101.112.193	ipv4.imgur.map.fastly.net	United States		54113	FASTLYUS	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	634965
Start date and time: 27/05/202207:38:13	2022-05-27 07:38:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	View Shared File.pdf
Cookbook file name:	defaultwindowspdfcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.winPDF@65/179@11/10
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.9% (good quality ratio 94.4%) • Quality average: 80% • Quality standard deviation: 27.5%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .pdf • Adjust boot time • Enable AMSI • Found PDF document • Find and activate links • Security Warning found • Close Viewer • Browse: https://webmail.serendahsteel.com/?locale=en • Browse: https://webmail.serendahsteel.com/?locale=ar • Browse: https://webmail.serendahsteel.com/?locale=bg • Browse: https://webmail.serendahsteel.com/?locale=cs • Browse: https://webmail.serendahsteel.com/?locale=da • Browse: https://webmail.serendahsteel.com/?locale=de • Browse: https://webmail.serendahsteel.com/?locale=el • Browse: https://webmail.serendahsteel.com/?locale=es • Browse: https://webmail.serendahsteel.com/?locale=ar • Browse: https://webmail.serendahsteel.com/?locale=bg • Browse: https://webmail.serendahsteel.com/?locale=cs • Browse: https://webmail.serendahsteel.com/?locale=da • Browse: https://webmail.serendahsteel.com/?locale=de • Browse: https://webmail.serendahsteel.com/?locale=el • Browse: https://webmail.serendahsteel.com/?locale=es • Browse: https://webmail.serendahsteel.com/?locale=es_419

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.4.250, 80.67.82.97, 80.67.82.80, 142.250.203.110, 74.125.108.200, 142.250.203.99, 34.104.35.123, 172.217.168.42
- Excluded domains from analysis (whitelisted): e4578.dscb.akamaiedge.net, clientservices.googleapis.com, arc.msn.com, acroipm2.adobe.com, r3---sn-1gi7znek.gvt1.com, go.microsoft.com, redirector.gvt1.com, login.live.com, a122.dscd.akamai.net, sls.update.microsoft.com, update.googleapis.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com, fs.microsoft.com, content-autofill.googleapis.com, acroipm2.adobe.com.edgesuite.net, r3.sn-1gi7znek.gvt1.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, armmf.adobe.com, edgedl.me.gvt1.com, store-images.s-microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:39:22	API Interceptor	12x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA8321101
Malicious:	false
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Program Files\Google\Chrome\ChromeRecovery\scoped_dir3876_980132676\ChromeRecovery.exe

Process:	C:\Program Files\Google\Chrome\Application\85.0.4183.121\elevation_service.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	259472
Entropy (8bit):	6.621401853828968
Encrypted:	false
SSDEEP:	6144:wgtABO5wl1poLsQXo2fJjazGDJvvLAOk7CWn5l4rB+5Jb:wgtAFB+sQXo2ZRG7CWnaB+5Jb
MD5:	49AC3C96D270702A27B4895E4CE1F42A
SHA1:	55B90405F1E1B72143C64113E8BC65608DD3FD76
SHA-256:	82AA3FD6A25CDA9E16689CFADEA175091BE010CECAE537E517F392E0BEF5BA0F
SHA-512:	B62F6501CB4C992D42D9097E356805C88AC4AC5A46EAD4A8EEE9F8CBAE197B2305DA8AAB5B4A61891FE73951588025F2D642C32524B360687993F98C913138A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;....zp..zp..zp...s.qzp...u..zp...t.\zp...s.izp...u.;zp...t.gzp...q.fzp..zq..{p...y.Ezp.....~zp..z..~zp...r.~zp.Rich.zp.....PE..L....a|b.....V.....|.....p....@..... .....vI....@.....Tl.....p2.....#..... $...\..T.....{]..@.....p..H.....text....U.....V..... ..`.rdata.....p.....Z.....@..@.data...d'.....j.....@....rsrc...p2.....4...x.....@..@.reloc.. $.....&.....@..B.....

C:\Program Files\Google\Chrome\ChromeRecovery\scoped_dir3876_980132676\ChromeRecoveryCRX.crx

Process:	C:\Program Files\Google\Chrome\Application\85.0.4183.121\elevation_service.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	145035
Entropy (8bit):	**7.995615725071868**
Encrypted:	**true**
SSDEEP:	3072:TdgEhmDf+E8VY0x81Rkc6L2oqzqkPEu30gZlc3G2ZknF:TyEhmDf+/+Fnkj6lEukgZyyF
MD5:	EA1C1FFD3EA54D1FB117BFDBB3569C60
SHA1:	10958B0F690AE8F5240E1528B1CCFFFF28A33272
SHA-256:	7C3A6A7D16AC44C3200F572A764BCE7D8FA84B9572DD028B15C59BDCCBC0A77D
SHA-512:	6C30728CAC9EAC53F0B27B7DBE2222DA83225C3B63617D6B271A6CFEDF18E8F0A8DFFA1053E1CBC4C5E16625F4BBC0D03AA306A946C9D72FAA4CEB779F8FF CAF
Malicious:	false
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....S'.....2.{....'....+.'.."..Y.x.ISa...)....H.&92..?!..~..F.5."...n,.B.-|\.)..(.....]G..j.-M)...C.....o&L..0.K.....UtP.&.N...;..^w/a{}v...~KG;...?.1...k.c..D.U.....J.6.`.G.5.x.k..[...i.A.@I^..I.<A. J...j.'.G.`.$q.N..Tdq]2]p.OF..#.#.....'....8.3.....0.."0...*.H.....0.....O..(...':19..O/.>....=.....m.n\.z..q.....JW..F.....+H.Z+KGO.9....8.....U...&.y....,$...?.Eo.....\f/.Z..+M8...B.3'..Y.r...X.AS?.~..k..n..... Z...&.G....."n.....l.0v.x#<....Lx,-.w..-..d.....J.pT..('e~*{%kQ.Q.....rI.....Z....v.N.....J.d_.....rX.....w@.b.[.c../V.'c...!.~.k..}z...U.S..nC.....@.....Y..#.D.z.....5&.1O...X=p..2.F..P.6yP..>{.....HBX.*.E5....y..

C:\Program Files\Google\Chrome\ChromeRecovery\scoped_dir3876_980132676_metadata\verified_contents.json

Process:	C:\Program Files\Google\Chrome\Application\85.0.4183.121\elevation_service.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1772
Entropy (8bit):	6.019907048086037
Encrypted:	false
SSDEEP:	48:p/hPGxBJ7akeSpKssMLgWuG7bmTkfhs8vox:R9i7aaKssMUWuG7biIQx
MD5:	35C7E305A06F30D3F0A97693C3504265
SHA1:	B30C965F53A93676CC9D87D29F5E6AC5B605DD84
SHA-256:	3B6FB2683B4DFD83FDD0C6EE096F378AA85C6B1ACC73EC66288802A71C9381F7
SHA-512:	A6AC0DDC3C99D59A2C667410FE94BB8F267D1CF422C337FEBCFBAE23D5C965B0E965FF0B77FC88FA9E7B06EE6CE6D532B6ECB0D87A53FB282260EF812379EB7C
Malicious:	false
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJDaHJvbWVSZWNvdmVyeS5leGUiLCJyb290X2hhc2giOiJVUTRsOWhOY3VCS21lc2Utakd2ZE52X1VCWXFTTWNpTGZQM3pxZ2tnXy0wln0seyJwYXRoIjoibWFuaWZlc3QuanNvbiIsInJvb3RfaGFzaCI6IjBhd25UUEVCZ0NEeTJXTmFVWTdSb2ZJY3dzdnA0cVE1THNlUzFVdGJVdjQifV0sImZvcm1hdCI6InRyZWVoYXNoIiwiaGFzaF9ibG9ja19zaXplIjo0MDk2fV0sIml0ZW1faWQiOiJmcGplb2FkbWdlZGFqcGxtcG9hYWprY2hkb2ZjbHBrZiIsIml0ZW1fdmVyc2lvbiI6IjEuMy4zNi4xNDEiLCJwcm90b2NvbF92ZXJzaW9uIjoxfQ","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"ef1pxaTj-_-MaYe95eLdl4WHEPJq4PB7n1seVNh9AxlAGhDeKZD2PDPdzEYwLEXP6d3DCgNBaZDMZeByzQbRob9fSKBwHKzITZC0ScxWJTc8DuWlYfQdRMTrzxr_7S1FVvRx4Fxi7FFg921RIa7d2zXCGnA8qIvfUzYBU0TYoMeo--GC5JmJGpwrDi_9Xq0saxXUViu8o7Vlbul2ZEFLNMpHSfafBFLJVD_0cJc5arSdhdEVdAW1MztVSQ8CFfKhci2LBn3fKihN2_klwBKfbfmzKNm5aLoOf_iG3hjIoLji8dcxYo5sYXugJENpRrs-_AclQKykKKuD8wi45RK

C:\Program Files\Google\Chrome\ChromeRecovery\scoped_dir3876_980132676\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\85.0.4183.121\elevation_service.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	4.682333395896383
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFJ9LAG9Xg0XTFHqS1wP/pEeSWU4pv/8F/FxLj2RF2fcTZTotL:F6VlM90ggITgS1wnuWfB0NpK4aotL
MD5:	7A8E3A0B6417948DF4D49F3915428D7A
SHA1:	4FC084AABDB13483567D5C417C7ED8FD16726A80
SHA-256:	D1AC274CF1018020F2D9635A518ED1A1F21CC2CBE9E2A4392EC792D54B5B52FE
SHA-512:	064D84A57B28C19AD10742859DA493D0826B47ADC632F6C623DFB4DE36D72A9D29BE98518061A9FFD42D99FCF01F27DE39CE74782B3A5ACBBE11DFDDEEAB59A1
Malicious:	false
Preview:	{. "manifest_version": 2,. "name": "ImprovedRecoveryComponentInner",. "version": "1.3.36.141",. "imageName": "image.squash",. "squash": true,. "fsType": "squashfs",. "isRemovable": false.}

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.622483124952709
Encrypted:	false
SSDEEP:	6:men9YOFLvEWdM9Ql1wup/ltolXi7Z+P41:vDRM9M1wS9eEZi
MD5:	81F74FDB5BEA3CF7A998DEBDB847C892
SHA1:	CF253068BB0F1BAA1D33E73BE3A1ED7110353D39
SHA-256:	5A39B3D099024D7C83183A12CCB66F788984B72FB0557DE6000590980E39D6E1
SHA-512:	CD5B105AA77CA7A4D674723236FD1A364BDA1E675D11C6E67C84E94C8A78632AFC9DA10FE7A6FB1A7B88AF3C46AD13E64232A405D73D583119F2EA6DF35BB3 9D
Malicious:	false
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ....>/....."#.D!.X.8..A.A..Eo.....t.....d.{v.^.G...d.W.:...P..k%..A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	174
Entropy (8bit):	5.562019634990087
Encrypted:	false
SSDEEP:	3:m+lF9NX6v8RzYOCGLvHktWVhl/lO9koyRktksllM98fZe/O+/rkwGhkg4m1:mi9NqEYOFLvEkvoltkz8Be7Ywcr1
MD5:	1E0BC7F27635531A0B7AA9A574B0A7E4
SHA1:	0710FA7BD0C53BCF3EB56B6ABFCEB077176C6CF5
SHA-256:	182F1DA4BDB57D705702DE36E1F579C0077D719BB964098A309FE2D2CC3B7E76
SHA-512:	20CC37AADC4889E44163E28D00E1779DFCB56FF1A73AEE51835513A18CD01325309769070FAFE1A23577787BD9B0F3688BD5DF9CF9EDFDFCE1576655630CB18 4
Malicious:	false
Preview:	0\r..m.....,...._keyhttps://rna-resource.acrobat.com/init.js ...p..>/....."#.DML..8..A.A..Eo.....*.....1.x.'.vI..*|Z..o...+.4....0..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.582357731570362
Encrypted:	false
SSDEEP:	6:mMyEYOFLvEWdVFLBKFjVFLBKFlQhu3n0Q9hltmt/RlUoSjGY1:DyeRVFAFjVFAFr0Q9jwtZlUo6
MD5:	2D537B3A08D11515BA6CA6974965C762
SHA1:	978EBE340430E5E46C3FB4CDC1910C87A4BCF411
SHA-256:	57AB84E525E3B2B165EEF48F6576735B405B60B90B01631C663D56C6F4FFA18F
SHA-512:	5631CCEF8F0C8FAAC9C4B16330B174C89F7989CA1EECD80759845DD436908C85D7C2D85BDB8A583F4899FE773A8F97C199AA6D0D60D65555D02316BB117F7F B
Malicious:	false
Preview:	0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .8C...>/....."#.D,.T.8..A.A..Eo.....L .....hvDO.N.t@.....n.*..... ....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.620903424093862
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RszQbKtLy/lt1duiWulHyA1:IbRkiDSOkLy9DdjWus

MD5:	E362E7116ADEBDB6D6D8A6C022BDBA7F
SHA1:	122C1884F541435DE0EAFE7DC171BA9DB8305CAD
SHA-256:	4DB88A438EFDB6290F16F721F58848329E9EA70B7A65AC673A241E448E2EC80A
SHA-512:	729EF18131431E8E71F175A970C5EE25E1D644A291B2AB35BB3B211FC392344E1667BAFA588476DCB0FC8D93432DD3D487FC5F0FA0E4FD97FD74D7A701B6E33D
Malicious:	false
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js ..j0..>/....."#.D.*.8..A.A..Eo.....m.....8 P..a...R..Y....7.@..2Dm{..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.591464183503039
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVu8Fw/ltpDVyh9PT41:pyixRuCS9/DV41T
MD5:	80364ACC887FA710E788BE9A4E5B6261
SHA1:	24EDCF26BD8CABE83B679E6727420B85B55CC912
SHA-256:	C9A70B6CA9649EEC56C4C8CAA1171B8A9C9A327058D0894350F4A888D9BD91EF
SHA-512:	8792340D3817F1E4258E9ECF415B4A06CEA0D9D87DD665643286E1BE5353FAA0522FCB744D969204DEB2072CEC3BE7BF60F5F8F8112E50C30C831D067227F18
Malicious:	false
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ....>/....."#.D..R.8..A.A..Eo.....K.....k.Q.....-_..y.....O...>..1....A..Eo.... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.6128509855629005
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQG+1qltFflV3ZIl6P41:0Rhkg1QXbZ
MD5:	41C465BC8A9926232139E001E5552AF9
SHA1:	D95A34CCCACE36A6E0E14531A28268761D28E699
SHA-256:	198F678267E1EF5D3C8E50136EFEB5CF98986B530D0D9BBF9CFDAF9000F05FB2
SHA-512:	1908F33659784BE248CBFEC61FDA0C350B10FF991DB5E6364C467E3001A3407D53C2908FEC3117E2956A37A632C5CC3BC4353B7225EA6A5A67D08A61A2FE197
Malicious:	false
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .....>/....."#.D1{;.8..A.A..Eo.....uGE.....].>....uUf..N...k.....c..l.A ..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.520158416596513
Encrypted:	false
SSDEEP:	3:m+lZd8RzYOCGLvHkWBGKuKjXKX7KoQRA/KVdKLuVkc/llly/yRkt+lltVcyxMtv4:mJYOFLvEWdGQRQOdQfR/lt+/jD6g1
MD5:	652FDE204034373D9F67A5CDF418FE79
SHA1:	1FF0691A09486E0E56C696B8F5FD9FAEEECFA26E
SHA-256:	A16932017601DDCE1A4467BE0296889EFF91BA5BD49C4519D64036685F768904
SHA-512:	9E1BFBDE1A0C7841925B8D5356393D081065113960FDCB9508B0347FABC22E6123C0E4F8E475D62E8CA2182C0EF33167A486A2ADF3C7241B4F210DE48B2A188
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ....>/....."#.D..R.8..A.A..Eo.....d.....c..y/L....|y.n..C/I.....X7-ne.A..Eo.. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

File Type:	data
Category:	dropped
Size (bytes):	179
Entropy (8bit):	5.547359186441073
Encrypted:	false
SSDEEP:	3:m+lLp08RzYOCGLvHkfaMMuVy/luh0koyRktVNQMWqg4nRb7om5m1:mOYOFLvECMLyMroltsuR/41
MD5:	2E3E48E3C2EE7406A46FF1DDBF53E853
SHA1:	150ECDEA1FA60BD7E928BAA1DD5000C5BFC8536C
SHA-256:	54B07A7B21BABEAE34CD060019606D6514AE2FFBE46FA4E7DE4B396BF9EDAEAF
SHA-512:	9867D68DA1DF601B79B6898766E5BC62D6FDBFA04C5A08604A5B736419D5E52D10B853D72E2D5E7E7C7AAADDACD92B5DCFCC181DFF051D430FE608A5EF64F5B0
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ...q..>/....."#.Dkc..8..A.A..Eo.....).8-.....y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\39c14c1f4b086971_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.639912178056806
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAuwqltLXUGm0bbsIDMGH41:XfRMdZXUVKsIZ
MD5:	B41A7A69CB7C09D61C43D1F02F409551
SHA1:	618C2C998CC86CC5816D6E25B4CC6646531EE371
SHA-256:	B00F2E4FB68829A6251B5D69DEEDA8B1B5DA22B8FFE950934B61D828A77D4F5D
SHA-512:	2C36C74E9040C77011A2C20A66CB6E4B9E4E8F138685E5C7F7E6546AA5FDBE91657865D600AB94E568F888B92F5E8EC0E5507CF58B1E4FCF05800DF17CD6926B
Malicious:	false
Preview:	0\r..m.....T.....^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js .1.'..>/....."#.Do..8..A.A..Eo.....Y..J.....`.....^....L>..Xa./.....C.y.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.480860177588224
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuJuA9hlt1ll/by0zBUKSAA1:pRnYj7ll/b
MD5:	A377E75ED7031E2ED6C17E255C80E296
SHA1:	AB59C14B663C27BE6888EDC6515C06EBEA111253
SHA-256:	2E6A30D313C0CE94E8120AD8FB60299D17F5295002A742EE34511B45B77A8FEC
SHA-512:	D8B6D6B32FBFBCED233D4DD22754B72089B1117BC6D55E09061F4B30D93623AB0A9DD07F5E2E179B570754E8D6EE91F0F260860E2B177D69998A4410414E275
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .c....>/....."#.D..b.8..A.A..Eo.....4.a.....Q..E.=....=h`t..t..3%A.F$..w..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	177
Entropy (8bit):	5.5302156452495375
Encrypted:	false
SSDEEP:	3:m+l64HXlA8RzYOCGLvHkjXMLOWFvGbul+OG9koyRktWtkd1dn76KohyP5m1:md4HXXYOFLvEjMSWFvGbLOfoltykjUd1
MD5:	0D3516ADEE33179633051684EC7D571E
SHA1:	B2CFEA34B7890105D735B9F3915B39D73C6C0455
SHA-256:	883FFE371B6309D44E35D90B24CE2804D9DFF749AEEF1852901977E94C684916
SHA-512:	4877D5339FAA2595BBE4F13EFF849E91FC5AD2774C37AC02943938566A2EF7752C20F75EAB943D9331B064A81C6A224240AD31ABCB598A97A44F902A4D4EE00E

Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js . .p..>/....."#.D.[..8..A.A..Eo.....PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	187
Entropy (8bit):	5.569300466292
Encrypted:	false
SSDEEP:	3:m+lpSUllv8RzYOCGLvHkWBGKuK2fKVL2k6b+/lTOyRktTDF7UPqf9tsDMaPV44m1:mkl9YOFLvEWsfOL2N4OltaPqVyM+VY1
MD5:	4C2AF592F856C805B5FAD2609F880C39
SHA1:	B2472494CABF1CE08A5EEAD376F001A514EAF344
SHA-256:	12B54A93CBA8992A279A06F7DCE6198D2D476703E43F4620D9057EF278332EFE
SHA-512:	C633C115F0E86F3F64CA950A2B2F7E4503364994920516150AF038DB2CAB7A32F5A4D1591A88711572CA47B25F84020119B860D31D31B0CED99C3FC7B6893722
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...~..>/....."#.DFy*.8..A.A..Eo.....q.O...j...._y..L^z...?..@N..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.620507343590825
Encrypted:	false
SSDEEP:	6:mt9YOFLvEWdVFLBKFjVFLBKFlyqFdQ/ltq6twSeKaT9pr1:URVFAFjVFAFdQ9M6twSeKaTL
MD5:	0339DE6F4C189F3603EB81F4A5472C8E
SHA1:	21D18DEDCCE6271B4A3B8D62107C92B53407C656
SHA-256:	76196DC36C63B2950F53C668C651FC7A9928D1A1AABAE8DF0F8842DFA7FCE97A
SHA-512:	8E0B0D7CCF890B14FD07C6C1E69FFDA1C99D18D736EEE1990F2F546DCCF0C50462F52386CDD3912A9197661F643E5557C50A15D755E363AC0400C684109E340
Malicious:	false
Preview:	0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js .W..>/....."#.D.Y\.8..A.A..Eo..... .....H...{...2../.k`..r4.C. .A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6267ed4d4a13f54b_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.565683448958373
Encrypted:	false
SSDEEP:	6:mq9YOFLvEWdzAHdQPUmpL0hltL7ct5GFCaa+41:NRMHdKCjJQt5Gda+
MD5:	20180AF3F595E5E0A31EA0C67FDCBD0D
SHA1:	F9CBE6A7EA9E4139B559C9A0936843538B79E00B
SHA-256:	343D696D562C41EF4D40FBEA0600C345BC4E2B74DABB6CCF2989564A23A6B916
SHA-512:	8A7ABE5FBBDE0FCCAE6CF5ECB43840CE36EEE859CA21281C8512994676A15C14C2379E52CAF7B2F9B921A722B4E3071E79F0C4C066247CF5594185BDAB2B8A 99
Malicious:	false
Preview:	0\r..m.....R....L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js ...'..>/....."#.D.1.8..A.A..Eo.....mh.....G.3D.....Q.g0...._.Q.....A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	211
Entropy (8bit):	5.518423690292056
Encrypted:	false
SSDEEP:	3:m+lx4F08RzYOCGLvHkWBGKuKjXKGBIEGdevA/KPWFvTqallYxVh0hyRktYnyrpYU:ms2VYOFLvEWdvBIEGdeXu52h0hltB11

MD5:	0403B856D7DAC358DE093962E5795335
SHA1:	EBF7662F0F1E820E91E52AF4107A1997FF808759
SHA-256:	6C8C9D758C87CBD06E373381ACBBFAD180502D74D61EE18261E7D6711411F057
SHA-512:	415A3BC7269C7AACE78308B0D77AD703A9F955E3C270A219480BF1F8A5B175BEA18860F7299CF706283F26252CF8378D3CA4B62EEB65D728E7119F4B54B8849E
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .6....>/....."#.D[.T.8..A.A..Eo.....wD.....A.o]@r..Q.....<w.....].n\....A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.661499283555183
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQxntlt9HlTxm7OhKlvA1:RbR16qnfJTxmJ
MD5:	59B2BF1DC4F5507A59797190F9ADDFCA
SHA1:	461424CB4F540ACF245284AEE0136D4D38347051
SHA-256:	215D68157B64C6F65399BE2458D1AB9368D44BB572C31325B2349867BCCE3018
SHA-512:	0A9E46E0EB37D741358074FDB24343BBDC1E34B83D746AA0F47D3E991DFA24CA7FDC0C6208400B36D878D88EFF969183284C51EF24D015FCA4F3CD8DC92A62 0
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ..?...>/....."#.D..9.8..A.A..Eo.....4T].....Tw.....(..b...EO....9.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.588242647239258
Encrypted:	false
SSDEEP:	3:m+lx2gv8RzYOCGLvHkWBGKuKjXKX7KoQRA/KWEKPWFv00NllL3hyRktXt9tddF5V:ms2gEYOFLvEWdGQRQVuxhlt99tddFt1
MD5:	F774C8195C2B6BBA45D9C7F5CD8DF730
SHA1:	1340B2D535D608DBAE03E7F7D896E2ECB486622B
SHA-256:	96C4183426DE41BA4CB89E224F202EF229AF4FE9900A9E64B02723D6201DCBB6
SHA-512:	13EB471D0BB6B8425938DF71AEBF02CA5E817CDE0F5BC9FD40CB2A2C236A1517883C1BA80508D9B52860EF175EF0C8ACFBE34B3B3AC586541C0F82849483B5 AD
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ......>/....."#.D..T.8..A.A..Eo.....f.....@..{o]...9o|..qY....T....{..u.b..A. .Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	206
Entropy (8bit):	5.5987148880388045
Encrypted:	false
SSDEEP:	6:mzyEYOFLvEWdrIOQh2uMdLqltfEt1S/1:WyeRlW2xuJEt1
MD5:	D708BA5C5755A4EDC034C56C3DEE4BB6
SHA1:	32EAEA45F92A581D779D24842A7EB139124B2375
SHA-256:	46772003BD07A3A91DA99C28D902B9282D6DB764C867BF2961895D50F179BA61
SHA-512:	052B78EE310047B2B57448A27E8CB4C71639A61F8EFE5ED334A6EB9D7645941D2B0041B1676B32CAF2EEE00DE9306C8AB4AF3E232EFFA01A806A34D769BB51 C9
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..X...>/....."#.D..1.8..A.A..Eo.....i.....t\a.....x5.'OuE.C..@.....x..A..Eo.... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.56331193783623
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFvFkw+/l0Og/yRktsolwJNqww6U+5y:mnYOFLvEWdhwyuYinltsolwrqwK+41
MD5:	8407A870BC42D2AE869872D880AA6598
SHA1:	33764580091AB9EE74A39C27F0D92D9C3FDB1164
SHA-256:	C74B5C07767ECCB140F68D5C39C7D0D55C21B3BBFE7440F74FA65CEAC66B83FF
SHA-512:	2D675A3148623B7BBF020D2EDCA0A012ED2BADFA331F565928E9FBDB70510D888F86D247200D403633A900861D2CC6DDE6C085B7711AD969497BDB9F395765B
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .\>...>/....."#.D..9.8..A.A..Eo.....O.....7...o..a=.98I.....(3.$G.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.588751090095904
Encrypted:	false
SSDEEP:	3:m+l26Xa8RzYOCGLvHkWBGKuKjXKeRKVIJ/2NAJVKH/KPWFvlP6lDcdQ/yRktTnxJ:mYXYOFLvEWdrROk/RJbuvcltT2fO441
MD5:	6BD0F21ACDA215BC3BB8CA6E1961E160
SHA1:	3B5C8605A7B90ED6F94E55AB5D27FB7893ECDFF9
SHA-256:	946E3EACCCFDC1F4432A13415910AB5FE947BA12FF4DAEA7A082D04299400892
SHA-512:	A1D2966056A6A72D5B47E36BF4888CCBDA5E589CD3BCA6D0FDE854E482E790ADD091C02A6BD405BE2CBA755EB5E2BA47B1758A81C1AF1526A0D986923FB73523
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..V...>/....."#.D.R1.8..A.A..Eo.....~..rw.+[....!.)?..f.U..(=.=.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	186
Entropy (8bit):	5.567305610867357
Encrypted:	false
SSDEEP:	3:m+lhD4ll08RzYOCGLvHkWBGKuKdTSVZb1u+/le/yRktn3zoIN1OFPL4m1:mmDEYOFLvEWXIvU/lt3zV1QPLr1
MD5:	00ABDA87186E9A75730A5A18C4ADE43C
SHA1:	E2C2C1739E66E32E6AB99D8CD405A9123D88D184
SHA-256:	6CA0BD855E6CEDBAECC86F41E084F482E8754093C7E72E1AEE426E37252F786C
SHA-512:	B90D37F5929AA6786E5695D4E4BE42C13E12BDC3ADC6935320A9A9F1C7D8A239EBC8EA8C833AE7EDACBAF366DB46A7CC96D103F727D2A0A64618CE46260B94C4
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...~..>/....."#.D..*.8..A.A..Eo.....{.....~]...%s..<...n.f..<.....1#..U..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.6299500216128555
Encrypted:	false
SSDEEP:	3:m+l+nq1A8RzYOCGLvHkWBGKuKjXKLNfKPWFv/rllluhV/yRktYPFM8D6EsEJeUm1:m52YOFLvEWdMAuVr4/ltYNMEvsEJ41
MD5:	2D861498E103BA4C6A1CE3530AEFD1A1
SHA1:	1F09CD44AD203F892E95A878F662235EB120E55C
SHA-256:	D7A8630D7F3C6826B6DDCEF6A921A4B1D404383A0540ED426F4B12470B5BC51D
SHA-512:	351345A1909541CEFA65A1D40CD23A776D44A91D4044F849545D447E3F48EC1592682327502DD2B217AEA325DA8987F86054B6B72C7B3F7BBDAA57EDFD8F5D4

Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..A...>/....."#.D..U.8..A.A..Eo.....z._a...'.v.....4p3..1.']...A..Eo... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.555902607196559
Encrypted:	false
SSDEEP:	3:m+lf1UldA8RzYOCGLvHkWBGKuKjXK9QXAdWKfKPWFv3gXllDkxAyRkt4ltGFoDbg:mYilPYOFLvEWd8CAdAuO8Altoyong1
MD5:	D1EF03A2E8CCC07F0F1D775B5D41A4AA
SHA1:	F749BE215EDC02A1C08319A081BBC8DE68D05C54
SHA-256:	DEA1E1CD1D75F8428374E64D96E5A94E82249BBBE2399C13DD1162C3D12804C6
SHA-512:	1CF2C62A84255069895421DCBC9142342D76B27DD5275160443AEE6FE9A5E574F8D3015D671C146ABB393F89AFD573FAE294CAC109DEF615161D54219A040E6
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..W...>/....."#.D.WR.8..A.A..Eo.....q.a.....c}.H7M=M..-.....Ix..R.l...} Rl.$q.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.596341428282603
Encrypted:	false
SSDEEP:	3:m+l18t08RzYOCGLvHkWBGKuKjXKeRKVIJ/2oKPWFvnjulqUx9qyRktx/dOe28WI2:mY8nYOFLvEWdrROk/IuEAltfN16wG1
MD5:	9972F4759C0187F3BD8407D1C60BEB1B
SHA1:	4FD639724EA5627B50689CD079EAB2BCE91C3FCC
SHA-256:	EB76A6861F0453EE122C7523C575028E21DE29429F17C8102DB60ED9BC278F3D
SHA-512:	CE648C28935A1CD31D9095E59A27A19E00A9A41047F0BB0351AC567A75C5DC4045E280484C252C175C42504AEB7BA5042C2A8F6556F4794218D0ADA52B6F05E
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..0...>/....."#.DF@1.8..A.A..Eo.....R,P.....%.k.SZ..~W.. ...:)'B..ad.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.648382840002618
Encrypted:	false
SSDEEP:	3:m+lstxt08RzYOCGLvHkWBGKuKjXKX+IAuAJVKjXKLuVZ+f/lAfUg/yRktnWPmJec:mLrnYOFLvEWdrIoJUQfWNltWeJIi1
MD5:	B9B9E3C12A1D95AA3B09A323DCAE39E1
SHA1:	3ADCE6B67EC2F312574FC12024B3C2A0B5463F9E
SHA-256:	271E090511DF3FE54B1B6D74397640A933418DC8566445458DDA9664DA18B70E
SHA-512:	190F48763C3A6B575DA13D59C63719640D7C9518EF54CEF1771AA4349F01257807F49A9C618ED0882F0AEB033DF098CD229445E7FD1861B179D498D396A96568
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .S....>/....."#.D..1.8..A.A..Eo..... .~l.....;"./N_.,.:C..2....9L.H...3:...A. .Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.554290450982171
Encrypted:	false

SSDEEP:	3:m+lQ/pqv8RzYOCGLvHkWBGKuKjXKX+IALKPWFvcM1uuI7gOqyRktlsHlln6mgmOp:mOEYOFLvEWdrIhuu2qltlsF5zgm2d/1
MD5:	27A801AA7D924666B619D6AAB7F30F9C
SHA1:	897DBC2CC96DEC0BB43C7D965EBAFBBA95FE184C
SHA-256:	A067CBF78FCC5E8B6793DCD65185FF4B928D73EA15D319210AB825A7337ED89E
SHA-512:	AC3BD136A44A5C31EB520F4F3A9B2ACA764E291FF64D31CBCB7FB45ADB46D4F4ABA46046233502CC256639700B9447F381636CB18E19D37887DAC45EF2E4E1A6
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .....>/....."#.D./.8..A.A..Eo.....pFu.....Z.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.545629384745137
Encrypted:	false
SSDEEP:	3:m+l8UElLA8RzYOCGLvHkWBGKuKPK7Cvv6utlod2yRktImeBiaQ562HvpMm1:mAElVYOFLvEW1K6Qd2ltRx56uvp1
MD5:	64F7A4A82FF490903D27D9422C4E6864
SHA1:	F072308D8D6B8005F6D619172176954FA622B2D1
SHA-256:	72FC93B5AF487F9560D04BE600126B70C0D87AA410EF11F193A7B00780B00359
SHA-512:	4EC59F7786EFFDF7F3261A5521744ECDB0A00340405C5FEAA1EDB7CC519972AE9DDDB26EFA0A68AF752E5FDBBF1FD54EC945DBA029E51E661CAB529D35882477
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .T.s..>/....."#.D:...8..A.A..Eo.....zE.....z?...SwC...^..y.....V..7R-O.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.63507043799817
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuP+Ohltvw//TUDLYtmOZn1:xRBJTOjdwwDcFZ
MD5:	57197A3AD81CDCE2B66B074FA4EDA0FB
SHA1:	B16B3EAFB76D4BC9E4DB38DF8E93AE5056B3A596
SHA-256:	B97332CCCF5887DC29DA9B71DAC8BEA8A2FCBC097E5428860A1625143A966A06
SHA-512:	86464001D5D55B24EB832483EA051D1FA28C6EEE342C541AE91FDAB9213A95336E1C711D66EFE49F544AEE29CD9517CCF549CA09897316B96DF8196163D3B10
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .....>/....."#.Dp.T.8..A.A..Eo.....A.....t.q..W.EZ....1...[.zC.7mD..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.590755820854987
Encrypted:	false
SSDEEP:	3:m+lxCq//6v8RzYOCGLvHkWBGKuKCH6U4LJzWHK7WFvrswul/l1KG9koyRktz1H/B:msRPYOFLvEWIa7zp7vmoltz1HX8VPu1
MD5:	96856CCD53A8B8E8C8852493FF79FEE0
SHA1:	8F193E4364A21D13E5BA921C4A48EBCA3EE8AFF2
SHA-256:	099D388164ED836531D85F39EB9281796D6BF44EBEC506F93763923EC2FB1288
SHA-512:	4F3223A61467FDBDCB5FF4A7ACB4617E01869B3B171C0604BC0EAB5B29D823DB9CD95E37EA3793A5A352474E9514207933F4070F7F8CC40A6D3BD1C33EDED607
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..%q..>/....."#.D...8..A.A..Eo.....L...Im.@.....E.nW...IP..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.596436272538277
Encrypted:	false
SSDEEP:	3:m+lQi9lC8RzYOCGLvHkWBGKuKjXKVRNUpXKLuVBt/lcO3Q/yRkt996F4XVAZ+8cW:mKPYOFLvEWdENU9QgKnltSwiM3Y1
MD5:	8FF0F41E45BDE0FB1D27D15559C7D431
SHA1:	C4017706FE56A6D76AFE57F33E39FD2F2A6A8C62
SHA-256:	84A103C9171776631553424878 3FB02EF409E9421A7202CA21FD0F852126D7DB
SHA-512:	B1D0DB10D3E34BCE9CD69FDF70B067DBA1583B8CCEB798993ADB7B45A88C838BBF4C36EBC03932F40615793F717CE8E2DBF28DDD0722D492D39B26D25382AC8D
Malicious:	false
Preview:	0\r..m.....P...Yft...._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .....>/....."#.D..?.8..A.A..Eo.....g.....M....m+lS..e.....<7.U.P8*.0K.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.623405697896145
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQ6udohltGOjBRCh/41:XRc9v/j1Di/
MD5:	A64E3F7A2E52BDDE7896F1CDFE625AAD
SHA1:	A28F66AE30572EB97EB9D8C53DBCFAAE33F605AE
SHA-256:	3B02DC2D85F6E59423CFEDED6C1673C4F373C455057B54E9BF618B3045A507D5
SHA-512:	0AC16DB532E95E915721CA0816BD9A76382BAD3BB4FF9F79A72AF77B0E48F283B57719DE1D25DFE70AB179C8CF097F61A8305B948343E1A8FCED2ED4B806D5C1
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .4..>/....."#.D.5`.8..A.A..Eo.....y..<.....PJm...0x.x..RD...BB!@5..<..]...A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.590419374782984
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhu+ulFltZlkULlF4r1:bs6xRkiz3l7LlF4
MD5:	C0A5F6F076B0AAF93632990E4264EC79
SHA1:	445680CFB1F45CC694D060CF223B241575FA17DE
SHA-256:	59714A9F59C8213FCB775B8D16AC7CD655B5DB42D36893B1AD6C1D82163848C2
SHA-512:	B152EC5285AC218776D335FC7B250AB8BE053C15FAE70D0288968B16A3184C6464BD85E8B3FE4E2569CB7966BDF4D8A74B655D439A44AC4E8902C7CDF94E142
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ..$-..>/....."#.D"l.8..A.A..Eo.....*..|.....P...#4..l....5...5..).w.. .h.~..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.498308644639846
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFvekNll+ohyRktt3XECcu1isLK5m1:mhYOFLvEWd/aFu2ohltNEN941
MD5:	65F86527B128D11B6AC62B963B331BF7
SHA1:	AD32AA9745D80023BC2CFCBFFCCFD4CF0E8A8215

SHA-256:	2F24F8866E0006A82EB2647CD14F63B3534FCA0C900C0C900AC1A96B7FFBD61E
SHA-512:	268DF45D75FDE24D4F547C818D8CE3AC2A4EFA6681191DF9EF8850CB603751C060CCE7059688626539036DC73BB824FC162F85C1EB6D5870037467B3027359B
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .....>/....."#.De.b.8..A.A..Eo.....a.f.m.i.o.p..3U5.....^...I.A ..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.551453477588984
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VlGXOdQhXg/ltJLBMqVd3G4K41:2DRuRmQ9DLB9Vd2
MD5:	FE4D3C71132A5CCF175596D14D73D5FD
SHA1:	A5F4A55CD56587F95145861E1EC1921266738050
SHA-256:	7864D47F2B1A649FEA485139F7D3B43464F0EBBB8B4E57C8D67F6E4C8CD6B5B8
SHA-512:	CDCE3C18BECC0ED69D9BF9C6A169323F49644B25F3BBBFB8F2BC30F3C96C3B50B1EC2C08069F83AD6D1FEA8E6906781A255879B404EAE4D30A7514F58BE3D A7C
Malicious:	false
Preview:	0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ....>/....."#.Dr.R.8..A.A..Eo.....w.....y.$..$.v5j...T...z.]..._S....A..Eo.... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.558330666389947
Encrypted:	false
SSDEEP:	3:m+lQyu6OA8RzYOCGLvHkWBGKuKjXK9QXAdWKjKLuVmllMV8yRktLPW4ThzJuA4bx:mkqYOFLvEWd8CAd9QhlthuA424r1
MD5:	F685BC5A51AB4FB9C8BAE6C8CED30C1A
SHA1:	5ACCE6CCDB2DCF47782570D2ED2A5A5F90F4768B
SHA-256:	4063FE140A95C5D37D29BB5CB79732F888705FB647EF4960AEE4CBA7F20BB710
SHA-512:	14128B825E4002D54B449ED55E7D9B2E30B8351623B4999652EE26C46E6BE6737F9C57D29FD2EFE57EAA8B329A6577781746555B36F5227A4F4397ACF1AC0576
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .....>/....."#.D..a.8..A.A..Eo.....Gc!.....#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.602976353587929
Encrypted:	false
SSDEEP:	3:m+lS5Etla8RzYOCGLvHkWBGKuKjXKVRNUp/KPWFv10b+/l7Q/yRktF+TAg2iHio9:moXXYOFLvEWdENUAufLcltFlyC8n1
MD5:	48E4AA29ACA3D470BBD8A81D86A62CBC
SHA1:	1C256DB47E93C18F56588DFCD5E5FBD871F8A105
SHA-256:	58C48111EF15F958E4D5C32903ADEEFC01B09E1BFE7B69BE750BF4B31576B008
SHA-512:	31AE85C09AB2EB39A682026B3EF59F658B96C4EF9B54544190440B703A6141037DE13C18A0F73DBE9D9A3658DFAF12895EA8C1C425433F0B01C17EB07000EA6
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js ..=...>/....."#.Dd.9.8..A.A..Eo.....O[.....8.../...;.\\o....1.....+..A..Eo .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped

Size (bytes):	221
Entropy (8bit):	5.625721103896447
Encrypted:	false
SSDEEP:	3:m+lFNrs8RzYOCGLvHkWBGKuKjXKeRKVIJ/2kKLuV6bulsohyRkt5q/XsYWmYk5m1:mQZYOFLvEWdrROk/VQmhlt+sLmB41
MD5:	50C5B4BC2A18585C59ECD62BB5FEE5E8
SHA1:	2D48891FB95824002DDE871735CFBDFE6339AE25
SHA-256:	E0BDB71536EA47FE35CAF917FB01B1EC99E378A7F30E4C6C9A83587864119084
SHA-512:	FDFA052F0DDB8F3219DE22E9D1E5F7F41EF6635B364DD85D0944697227119197ABF4AAC7030A087FEA7521E18B8D93E32277D314DBF3ACC873EC8F4694634FF
Malicious:	false
Preview:	0\r..m.....].....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .....>/....."#.D2<2.8..A.A..Eo.....g..... ./.ev.....N~..6.b.....$ .j;:C...A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.581078590424192
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuZgVg9hltfflBdm9741:qxRc/u4jFflBdu7
MD5:	F547C6E5BA2561264B17AEB895FD89F3
SHA1:	E21820126F9CADA0507E87174FECE728B16A7E9E
SHA-256:	EFCBDDA418452A51A38BA4E5BDB6D0AD0303F687384C9BDBC35CF217E59D8C5A
SHA-512:	3840AA3DD24737B531E350682286CD611E3898139F4B3C2916A26995DC8D9FC73286162E26DE80B062D341AEF14C40048A2504F090569C403A855B772E1BA26B
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ..m...>/....."#.D..T.8..A.A..Eo.....r.Q.....U...I.>P...X...x..0U.~;m.x.k.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.538234340721392
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvowuljtyRktcGB6shoq+Nem1:mMOYOFLvEWdwAPVuWwQtlt5B6Jn1
MD5:	9EFFB29A75B7C58E6AF0683B5F6A5BCF
SHA1:	98D52F0AE2740A8087AAABCC5B6975F6A8F4C645
SHA-256:	845CA10A434CBE3FF8C16E1CF78123F9EC75D63D4442BF2EC32EE03026840C47
SHA-512:	B826A29D8DAEEAFE98DF70E14B738CF86099C136037DC900982ECE2501F374A1B2F793A05A8F76C6F3C3E2CCE98C0CBD3CF7AC70A19BA875873884A9CD4DBBA1
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .];...>/....."#.D:u9.8..A.A..Eo.....+ms.....k....F..D..O.n;[.1m.....=..A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.632650656790714
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQcG9k9hlttAhcsBXIh1:mxRBJQrf9jYB
MD5:	BEAA58D6A23A538DD995C8A3FE14554C
SHA1:	55C608C9FFE8C9951BBA12D7981A888652EE343A
SHA-256:	339DEC63B1231EA1A6D51EA47C45452851B9CD3B53A9AA634D4F4F6E9DD6AE3C
SHA-512:	70F823BB0C9719CAF003524BD08B3A8EA608E09EF9897F61CB9CF5A48A452C78178FD9EC3C0AD8B019E84DD6D771DEB0EE393F19E9D39681276D94FB06B7552
Malicious:	false

Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .....>/....."#.D{IT.8..A.A..Eo.....c.....k..`..N3.... ..d..$[.....{.A..Eo..... .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.58940181652529
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQdae6hltXrc3Me/1:3RrROk/syafj5r
MD5:	A153C44670AE9F01AC309D990F13B310
SHA1:	3A46BF6588CCF30FC2096D45F52AD8C37562B9E0
SHA-256:	6D1C57058A76DDD2A4453C8D90DA9D0671C7C885B00FA318F5CF76D71D24C315
SHA-512:	6DBC0F77AC9C86ED87FA02B7847CBC97D2D94F1E6375F603212F2A15499C024C65453B0B9D9A116CCCF926761857E4BC78268BFB460A1B1ED282B9CDFB3AA2 5
Malicious:	false
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .....>/....."#.D..2.8..A.A..Eo.....y%.....9Q].8O.z....= ..:.N.{....N{.A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1080
Entropy (8bit):	5.149234613228509
Encrypted:	false
SSDEEP:	12:/i8yVG+/l/Cui5tHLGh/bwKQFMzlkRQwUr+gi+/l/p1F/nGZmMvm91taZx42XdgL:q8QUugkFwKKMiTU15P1taw973
MD5:	E0E12A2D5ACB323F81F99448C0E316B4
SHA1:	D21639C1CC40D99782EC4FB39214DBBE57B5DFAD
SHA-256:	785F3BF41501F6D833C08F3ACD21F72A97666766E5EA7C6A88BEA4D18FF005AE
SHA-512:	B8E900A58036FD116D42CFDFF98B8FCA5605BE64506547A26563B204C0F219109EA1DB307696A276C0D6C96C0DFF1AD86F585EA06F2F40847451F03B88429851
Malicious:	false
Preview:	0....y.oy retne....+.....V.....*...pt..>/.....;.y~A..pt..>/.....oB*.-e..>/.....#...(...A_./.....D.4.@....>/.....[.i..%.@....>/.....k7A..pt..>/.....]...I..$(..>/.. .....,+...._.#@....>/.....<...W..J.-e..>/.....J..j...@....>/.....6<|....-e..>/.....2q.....pt..>/.....P....V.pt..>/.....!...0.o@....>/.....P[. q@....>/.....3...@....>/..... .v...q...pt..>/.....a.....-e..>/.....C..M.....A_./.....qi.K.L.9.$(..>/.....K..JM.gb.$(..>/.....$(..>/.....F..=z;..pt..>/.....o..pt..>/.....Gy.'.h..pt..>/.....:..N.A...pt ..>/.....;/...@....>/.....@....>/.....^.~..z.@....>/.....+.{..'@....>/.....@..x.@....>/.....MV3..@....>/.....A?.2:..@....>/.....q.@....>/.....u\]..q@....>/ .....o..k..@....>/.....*....@....>/.....+.U.!..V@....>/.....~.,.4>.@....>/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	1080
Entropy (8bit):	5.149234613228509
Encrypted:	false
SSDEEP:	12:/i8yVG+/l/Cui5tHLGh/bwKQFMzlkRQwUr+gi+/l/p1F/nGZmMvm91taZx42XdgL:q8QUugkFwKKMiTU15P1taw973
MD5:	E0E12A2D5ACB323F81F99448C0E316B4
SHA1:	D21639C1CC40D99782EC4FB39214DBBE57B5DFAD
SHA-256:	785F3BF41501F6D833C08F3ACD21F72A97666766E5EA7C6A88BEA4D18FF005AE
SHA-512:	B8E900A58036FD116D42CFDFF98B8FCA5605BE64506547A26563B204C0F219109EA1DB307696A276C0D6C96C0DFF1AD86F585EA06F2F40847451F03B88429851
Malicious:	false
Preview:	0....y.oy retne....+.....V.....*...pt..>/.....;.y~A..pt..>/.....oB*.-e..>/.....#...(...A_./.....D.4.@....>/.....[.i..%.@....>/.....k7A..pt..>/.....]...I..$(..>/.. .....,+...._.#@....>/.....<...W..J.-e..>/.....J..j...@....>/.....6<|....-e..>/.....2q.....pt..>/.....P....V.pt..>/.....!...0.o@....>/.....P[. q@....>/.....3...@....>/..... .v...q...pt..>/.....a.....-e..>/.....C..M.....A_./.....qi.K.L.9.$(..>/.....K..JM.gb.$(..>/.....$(..>/.....F..=z;..pt..>/.....o..pt..>/.....Gy.'.h..pt..>/.....:..N.A...pt ..>/.....;/...@....>/.....@....>/.....^.~..z.@....>/.....+.{..'@....>/.....@..x.@....>/.....MV3..@....>/.....A?.2:..@....>/.....q.@....>/.....u\]..q@....>/ .....o..k..@....>/.....*....@....>/.....+.U.!..V@....>/.....~.,.4>.@....>/.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text

Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.253501879805395
Encrypted:	false
SSDEEP:	6:AX0Aq2PWXp+N2nKuAl9OmbnIFUtqVfX0eZZmwYVfX0TFBFkwOWXp+N2nKuAl9Omt:AX0AvaHAahFUtiX0eZ/IX0TF/5fHAaSJ
MD5:	05BBDC07D22AB6C5A1982BBDF8649E01
SHA1:	448BEC224FDACF69EC97104D8A5E78F1A8A5F3F1
SHA-256:	2C08AF5866335052566C23887EE748B3A38F29D24DAB1F50E33A8674F6A55DF1
SHA-512:	AAFC7D274BA8900F926E38187AD29127522A272340A37750CBBE18482BD5955F4F70168153CD82A70C952271725F1956D055D078055FECC8F0A91ED2CB5A0703
Malicious:	false
Preview:	2022/05/27-07:39:28.165 1a04 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2022/05/27-07:39:28.173 1a04 Recovering log #3.2022/05/27-07:39:28.174 1a04 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old (copy)

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.253501879805395
Encrypted:	false
SSDEEP:	6:AX0Aq2PWXp+N2nKuAl9OmbnIFUtqVfX0eZZmwYVfX0TFBFkwOWXp+N2nKuAl9Omt:AX0AvaHAahFUtiX0eZ/IX0TF/5fHAaSJ
MD5:	05BBDC07D22AB6C5A1982BBDF8649E01
SHA1:	448BEC224FDACF69EC97104D8A5E78F1A8A5F3F1
SHA-256:	2C08AF5866335052566C23887EE748B3A38F29D24DAB1F50E33A8674F6A55DF1
SHA-512:	AAFC7D274BA8900F926E38187AD29127522A272340A37750CBBE18482BD5955F4F70168153CD82A70C952271725F1956D055D078055FECC8F0A91ED2CB5A0703
Malicious:	false
Preview:	2022/05/27-07:39:28.165 1a04 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2022/05/27-07:39:28.173 1a04 Recovering log #3.2022/05/27-07:39:28.174 1a04 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.010978819626460943
Encrypted:	false
SSDEEP:	3:ImtVdXb+j4x9pPlXlpyPll//zVrzlltD0lGQZ7XEZhGIelHdP4/X:IiVtg4x9pdM//hFwl570ZhdelG/
MD5:	E36F8F81D3C03F6AAF7D768706B7673F
SHA1:	EECE93F9E417717892E50F6A159516DD76C255B0
SHA-256:	C6E687FF9677244574F37AD2877726DF64E5BAADDA2ABE8C4759BDE8344E44F2
SHA-512:	0582ADCFA1A09095D4482C9A61475C8B77FF444BF2655DE4F6583BBB2699A054BBB2292DE2741FEEB27AFE0835B0B48F476418EE1A666DE20CA146D1EB4390A4
Malicious:	false
Preview:	VLnk.....?.....Tq.>..j..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-220527154329Z-214.bmp

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 152 x -152 x 32
Category:	dropped
Size (bytes):	92470
Entropy (8bit):	2.842806359383282
Encrypted:	false
SSDEEP:	192:6F/UMZTMOdG6mLVJG3XdYajBgVarfEBMvE:7GBUpVQ0M8
MD5:	9314D7F42BDA381A1111C7C33A4F0CFA
SHA1:	39A277F76F4DA347BBD2C462BC6ED651733F91B4
SHA-256:	2DC1A7A21260DF85C3AEB4DEE4AA7210D79489138F3956F4D70075D3EEF61D59
SHA-512:	A9DF1E50C927065721F51516ECA6EF294CDD21AF2E3029BDDDC9E7F640AADCB03CE0320D99F7985FEE2FBE7427A649DDA7A2BC43581676F098ACF674B74A0806

Malicious:	false
Preview:	BM6i......6...(.......h..... ....$.................... ....$... $...$. ..$.......................x...\...[...[... [...[...]...k..

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000
Category:	modified
Size (bytes):	61440
Entropy (8bit):	3.5652640874849104
Encrypted:	false
SSDEEP:	384:3eI9dThFtELJ8fwRRwZsLRGlKhsvXh+vSc:9kYZsLQhUSc
MD5:	619E53B728FE5A541CB4B4E982BE78A0
SHA1:	AF4889F67686FDECDF16575B67C4CFF6563BFEC4
SHA-256:	1152AA2084A1AA8FEB4156BF5C60A9E22B9182E2477A3D83B74662D1806153E0
SHA-512:	96F936F82701890D291CB3AD1AD83E989E292824521A51D6D147DA67E7DD695CB20DB18F0A861055B6263993341DFE5C0F49C14DE6214200D1819723976F9A88
Malicious:	false
Preview:	SQLite format 3......@ ....$.......1........T...U.1.D.. ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite Rollback Journal
Category:	dropped
Size (bytes):	8720
Entropy (8bit):	3.2872752275677253
Encrypted:	false
SSDEEP:	48:7MBom1C1iomBiom2om1Nom1Aiom1RROiom1oom1pom1tZiomVsiomgzNqQlmFTIT:7j1uOhtCszNN49IVXEBodRBku
MD5:	522D60B48F31CE05D0626A207913F354
SHA1:	826F8B95A7758557079BD0915675E215DC278ED9
SHA-256:	9D2CA0A61C879C86256E5CA1C00351CC9F4242F59D55AD0D3CBCC1CB66D69487
SHA-512:	2E7692D4E18807DEB83E34ED805B6CED8A13A893544E0876C85B507858FD68618A2D5EAFB09C45CD7BEAF5793F5C1B4236A18CB16BEFD9833E46F6E0FC2DE9 27
Malicious:	false
Preview:	.... .c......yT...s....... .L.s.y..

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5236

Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157443
Entropy (8bit):	5.172039478677
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3+2:RNj3aRlQShhp2VpMKRhWa11quVJX2
MD5:	A2C6972A1A9506ACE991068D7AD37098
SHA1:	BF4D2684587CF034BCFC6F74CED551F9E5316440
SHA-256:	0FB687D20C49DDBADD42ABB489C3B492B5A1893352E2F4B6AA1247EFE7363F65
SHA-512:	4D03884CA5D1652A79E6D55D8F92F4D138C47D462E05C3E6A685DA6742E98841D9C63720727203B913A179892C413BFB33C05416E1675E0CF80DA98BE90BA5E4
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName:Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst (copy)	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PostScript document text
Category:	dropped
Size (bytes):	157443
Entropy (8bit):	5.172039478677
Encrypted:	false
SSDEEP:	1536:amNTjRlaRlQShhp2VpMKRhWa11quVJzlzofqG9Z0ADWp1ttawvayKLWbVG3+2:RNj3aRlQShhp2VpMKRhWa11quVJX2
MD5:	A2C6972A1A9506ACE991068D7AD37098
SHA1:	BF4D2684587CF034BCFC6F74CED551F9E5316440
SHA-256:	0FB687D20C49DDBADD42ABB489C3B492B5A1893352E2F4B6AA1247EFE7363F65
SHA-512:	4D03884CA5D1652A79E6D55D8F92F4D138C47D462E05C3E6A685DA6742E98841D9C63720727203B913A179892C413BFB33C05416E1675E0CF80DA98BE90BA5E4
Malicious:	false
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName: Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1, Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Ar ial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength :1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName: Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Ro man.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

C:\Users\user\AppData\Local\Google\Chrome\User Data\012888bb-c034-47e7-85c9-9ec290c4c908.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	206867
Entropy (8bit):	6.072456123356235
Encrypted:	false
SSDEEP:	6144:Ex7cFfKzNM+gc+VLb8eA5wc5CaqfIlUOoSiuRp:E5lG9c+VLIJ515Roq
MD5:	CE8D4C4996DCED7AD6F13B733D3F5F58
SHA1:	FE5EDF4DEAFAF9F050B319C743BAAFB177F69588
SHA-256:	E2F8AE3C6850BA0E9C2E5EA2C254071D8449962E7309180FBBB86BB7AABB1218
SHA-512:	7FB8A47883F2867BF49B1832A886530846F298F2BFC92F7E0392A44575121A4D430514E448B51D5DDDFE3CC63324423ACEFF0893B14783A9CAD25003FE1A2AE7
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground": {}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"ne twork_time":{"network_time_mapping":{"local":1.653662463950412e+12,"network":1.653630064e+12,"ticks":222930665.0,"uncertainty":3243168.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrY iwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYq Qj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\05f23d1f-dd2a-42bb-95ee-de240b72b0a7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	198594
Entropy (8bit):	6.044457879375504
Encrypted:	false
SSDEEP:	6144:e7cFfKzNM+gc+VLb8eA5wc5CaqfIlUOoSiuRp:SlG9c+VLIJ515Roq
MD5:	A8961A1D4AEB2AB8ECAA02A530C36659
SHA1:	45E3EA6D99FA70EBACA0EE8B90A354D22C370B89
SHA-256:	0205760CF836E76248623FD42C9C08A8BF46B90A390B25BB47C9E8E7F3FC882E
SHA-512:	CAFD239F8333F33C2FB8E1EE5104132BFD88D7355E7E6AAC1FE6D2EDB7D38C1CA1E0170649C6787DCDE04F460F96C20E7908B11E29B1CC32F3F0352F779040 A
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground": {}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"ne twork_time":{"network_time_mapping":{"local":1.653662463950412e+12,"network":1.653630064e+12,"ticks":222930665.0,"uncertainty":3243168.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrY iwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYq Qj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639747675"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\1e97ddb5-9b94-4d11-8e3f-d8e111e13618.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7463671524236304
Encrypted:	false
SSDEEP:	384:xTfE0W5jytuIVxDg7N8rdv40330SbHmzGzWrRmcGx3qaqtrpMm9xr1WE4o7O2aY7:9WylJyCQH8evqAi0vfuIKmgQhl
MD5:	767E7FE20DE9BB30ABCDCE45F5A91851
SHA1:	8951BE2355839F67C7B8D39696C1E2F96DF35ACE
SHA-256:	FD5909C74E7493190CF0EE117C55809D855DAAA3450CE4C1B7C8DCDC8D4F35CE
SHA-512:	4CF44651A2122E20F3308BDF4AAC4F158F33BA8FDD78F5FB31B6BDF6DAE1A9D9271183D04F823EF363B01DB68A9713B1E2BDA1B51E6FAA6B546BFDC76D2240FD
Malicious:	false
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...f]8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\2c5d1626-74eb-4396-b376-532bf38e430b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	206868
Entropy (8bit):	6.0724552080141345
Encrypted:	false
SSDEEP:	6144:lP7cFfKzNM+gc+VLb8eA5wc5CaqfIlUOoSiuRp:lTlG9c+VLIJ515Roq
MD5:	22CBF73B2EFC71FEEEFC448E4280CB2E
SHA1:	56AF92A0402907C99DC65ABE8DE51B0C79A34B8E
SHA-256:	3239B603647B81543765DE1F42523B628958B0E6F174991BC43F5A82B25E732E
SHA-512:	02D96F4C61318F3F8BE8939B6DCCFFFD29CAD08DCAD66CA89D2BD16D920963E1A69328B986090FCA890C60101FC721AA5F0D1E088FED6E649E991B8B1C8029
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.653662463950412e+12,"network":1.653630064e+12,"ticks":222930665.0,"uncertainty":3243168.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\61177bf4-3adf-4556-94e5-07fc74310034.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	206868
Entropy (8bit):	6.072456152885985
Encrypted:	false
SSDEEP:	6144:ZP7cFfKzNM+gc+VLb8eA5wc5CaqfIlUOoSiuRp:ZTlG9c+VLIJ515Roq
MD5:	3EBAC34E799F7FF73CE46CF52CBE2BBD
SHA1:	C05F72C07A2F95FF1AF5EAD38B9D46F741BCD325
SHA-256:	05C32FC9D628C7A9F45DF0295651A1C1F534F86D3C7C424CA25FDEACCEA84D05
SHA-512:	68C20EE58790900C03A24BB493D96ECD7A1C7709C2C95A9F829DA33DEBB52FF23FD39EAEEC1D7B11C5AC0671403E6BE04EDC4C6C0018126732193D65C57EBD5
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.653662463950412e+12,"network":1.653630064e+12,"ticks":222930665.0,"uncertainty":3243168.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\6b2414f8-2abc-44f5-831d-8c2d23611ab1.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	198500
Entropy (8bit):	6.044205650654333
Encrypted:	false
SSDEEP:	6144:a7cFfKzNM+gc+VLb8eA5wc5CaqfIlUOoSiuRp:WlG9c+VLlJ515Roq
MD5:	5EE04A415476E6836DAC6BDD0A68F6A9
SHA1:	9CB4A806A96A5EB13106136510539CE9B0272C90
SHA-256:	0CEAFAFD3B7769CC89A6C50B6CF41799C5C93C777B282BC1033F32DFE47D5C2C
SHA-512:	300AE01C38FF51FAE18A2D6CEF5120929656FDAD06E4C81EC694C69540CF32552651D0E1059C1B66601E48F468DBF49DBF605766763B2F2FDFEF134C57576150
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.653662463950412e+12,"network":1.653630064e+12,"ticks":222930665.0,"uncertainty":3243168.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639747675"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\82b72114-359e-496d-b51d-69ea4390266f.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96052
Entropy (8bit):	3.746522361045131
Encrypted:	false
SSDEEP:	384:hTfE0W5jytuIVxDg7N8rdv40330SbHmzGzWrRmcGxOUqaqtrpMm9xr1WE4o7O2ai:NWylJyQQH8evqAi0vfuIKmgQhb
MD5:	79BCBAB582F0670623795488A0D8246D
SHA1:	642E48422368EC7DFD02EF41E7B09E06CCEC1916
SHA-256:	FE0FA9BB0691AED0858083CFB5B836727A582DB523B94412D5CB617BD91BF74C
SHA-512:	C3056A955896AFFF6D345422B6E71061C98FA797C14AF01927898A2005E83661FECDB8B030BC02D95CB5EBD2BF4F525BCD7E6AD59EA713EC78021850F7EF1390
Malicious:	false
Preview:	0w.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{}...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...f]8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\9a6ec8ea-05b0-47a9-813f-add56c12bd69.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7460293826189384
Encrypted:	false
SSDEEP:	384:/TfE0W5jOuZg7N8rdv40330SbHmzGzWrRmcGx3qaqtrpMm9q1WE4o7O2aYNJ1UdX:dylJyCnH8evqAi0vfuIKmgQhq
MD5:	FE47E1C4CA9283A44F234A0A4FD95828
SHA1:	F7FF84454D1EE51BF120CBF401FD707CCBB35AAF
SHA-256:	4A105564E30F3930D1F0B477A4642D53CEAA2A394F652A9A335E9AB268C1E632
SHA-512:	F978774C0321C6D816F0222737D6016AC6C7F445B1F9A30351BA62E4168C84AD89C9AA9844304288E1EECFF14AD21286AB4A29C4C73613C992DB83824C5856B6
Malicious:	false
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{}...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...f]8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1n:+ftlE1n
MD5:	BD4642AD6C750A12D912B20BCB92E14D
SHA1:	C549F0F48FDD4FBC62E51AC26D7E185160CE2123
SHA-256:	4FD71FE78DFE203137C89C9FB0734358FF432F2BC83338112DC7B830F9B30F2C
SHA-512:	04410D12EF327614C3AF1251C9906BFEB2977211A7F53CBB08A8C01F9465A382CD001E51AB936A0D196D359F1DECDDAEAF5E7D1DBD49CE5F4FF91BF5C332B6CF
Malicious:	false
Preview:	sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\489464f3-d7d6-4730-89cc-46a1e014e96b.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	2032
Entropy (8bit):	4.901556333062161
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDH3qyvz5sPhGsPrRLsPLPESyBsPlMHYsPYMHWbG:JTnOCXGDHa+z6V1MGwGWS
MD5:	25DE2FB0546CC1E5FD5F731E88AFB746
SHA1:	B1FE80DAAB8748B0A708137BAF3E69816687D0C8
SHA-256:	9EF8877344F28C68CB844C60CA2B7546A53115AE2907FDE7D9C0F5DC29E22ABC
SHA-512:	2E87E6683B0C82CA9DB7C98B3A15DE0446DA4B7CED97C72934CAE4A16123D915FC7B438A2EA101598E30DED49D37D32BAF83F1F3B88BD5B365482E12B3EA1D4
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13300728064551838","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\60544900-fd59-4ac3-b61d-5b07ee4fe0b5.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7c4ab1c3-bb89-4ffd-be01-80d6ebc791dd.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17529
Entropy (8bit):	5.57437988325648
Encrypted:	false
SSDEEP:	384:MwHtxLl+AX21kXqKf/pUZNCgVLH2HfDarUAjjPrH4G:TLlJ21kXqKf/pUZNCgVLH2HfGrUAjTrd
MD5:	0A28EF9B32420B46714CBB41417A9820

SHA1:	7FC594074B06664742D56B35BE951743018ED9B3
SHA-256:	3761F65AABF4467B4225AED0926B842E2665353112F520DD583CCE7BDDD04972
SHA-512:	9D1F99F358669AB68F94BFFA2AC8F8E90F2C87BEADF891B8A09AF9C1451A0559EDBF41E90AF6147A0AF31DA21D95FC876E6064149DFBBDC0E4986CCE5CC056 B4
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13298136061753412","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9201d6f7-b73e-4a17-9370-924f601aeb69.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871755235889535
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMZ:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhS
MD5:	AE133C52F86E27CD225F807F1DDB33A3
SHA1:	A0EB1D7B7D41F31993C975A8B5F27954F90B6DF8
SHA-256:	A795DA84B0B14FD651959C4E712B297CA76E50FAF03E18469336F5FB1BE5420A
SHA-512:	098D9CC2B0436B77AE03D9289C2DBF2316B0F0145C7AEE81F8F19A26964AB7F975F941CD2A9E14783E600602A195ED60A059B0EFEFFCEEC2BD0C5923E09663E 3
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9895fc68-2e53-4b0c-b28b-e5d40f4092fb.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5345
Entropy (8bit):	5.002683377198747
Encrypted:	false
SSDEEP:	96:nyBCcci1pcKIZok0JC3RWL8NkI1EbOTQVuwn:nACm1pc643YAkI4
MD5:	F081802DCABB0C4EE77A4EBC0E3DABFA
SHA1:	398A78025C4F0EC5D2873311871D59AACEC2E142
SHA-256:	2B5A1377528AA6AD44AC6761AFD8BDCC3A51347061A05522CF8E6509B0DC0EE3
SHA-512:	313BEC05064B3F762E1600E891C4C18ACE2F7C69C2EFF819CB42F5A37662DE4866BAAF2FBA2DE5630C95F1B4E673D2BFB7F429702CC081CD8C5FFF457208E6 F
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298136062885541","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT

MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvuI11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlXNQxlX:qTCT
MD5:	51A2CBB807F5085530DEC18E45CB8569
SHA1:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985D
Malicious:	false
Preview:	.f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.296664871787491
Encrypted:	false
SSDEEP:	6:AX0sIq2PWXp+N23iKKdK25+Xqx8chI+IFUtqVfX0sTWBVXZmwYVfX0sTWBVFkwOx:AX0rva5KkTXfchI3FUtiX0+GVX/IX0+h
MD5:	6892BF87D4D6027F78032765F8757C76
SHA1:	C07C2065E2F36E0D0EE476AB48F59AD7531CE453
SHA-256:	DDEAB1CB569CCB73E9C5D40E999C965B66F3DAE3C3C6D95031C95AF73F9464C9
SHA-512:	20A11B165ED61ECA6860E9C8282FD6AF01CDD71186915C384BCDC5D020C83C6FA9CB1710318549A0C4552A49C68770BD9822C17DB6A47E58667C01677EB099
Malicious:	false
Preview:	2022/05/27-07:41:11.954 13d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/05/27-07:41:11.964 13d0 Recovering log #3.2022/05/27-07:41:11.964 13d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.296664871787491
Encrypted:	false
SSDEEP:	6:AX0sIq2PWXp+N23iKKdK25+Xqx8chI+IFUtqVfX0sTWBVXZmwYVfX0sTWBVFkwOx:AX0rva5KkTXfchI3FUtiX0+GVX/IX0+h
MD5:	6892BF87D4D6027F78032765F8757C76
SHA1:	C07C2065E2F36E0D0EE476AB48F59AD7531CE453
SHA-256:	DDEAB1CB569CCB73E9C5D40E999C965B66F3DAE3C3C6D95031C95AF73F9464C9
SHA-512:	20A11B165ED61ECA6860E9C8282FD6AF01CDD71186915C384BCDC5D020C83C6FA9CB1710318549A0C4552A49C68770BD9822C17DB6A47E58667C01677EB099
Malicious:	false
Preview:	2022/05/27-07:41:11.954 13d0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/05/27-07:41:11.964 13d0 Recovering log #3.2022/05/27-07:41:11.964 13d0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1121
Entropy (8bit):	5.539351854743676
Encrypted:	false
SSDEEP:	24:6MIBXlb6AD3so6vXFNXaJQ73ie4DszdhUsGzq2dHKTAOxo7nQBrkPLpIpAblC:6MIF7HyFNXaJMYOhgdetJkTapOlC
MD5:	5DB78E720AF8478D95FA0B2DA2607202
SHA1:	D2D84BE0D9984911F2722E830C4811F489E2EFCA
SHA-256:	76A9E486E12406D619BF1DD75EABE4DA2ECC59B7EFB0D6582613CEF1F3CD03F2
SHA-512:	C5EB1B916F06CAC58F810F3AEA8EE1455AF105C946D073DF2726D188FAAB2DB9B7A4E97DA2E9E7A39F870E3CFE5F548579C646DB9E24D12D1A0233D07EEB5 E6F
Malicious:	false
Preview:	............"......arthurperush..com..cpanel..css..documentonline..html..https..login..sharepoint..webmail..bpkbsaya..http..includes..php..redirecting..v2..wp*........arthurperush. .....bpkbsaya......com......cpanel......css......documentonline......html......http......https......includes......login......php......redirecting......sharepoint......v2......webmail......wp ..2.........2........a............b.........c............d..........e.............g.........h............i............k........l............m...........n............o...........p...............r..........s............t.............u.......... v........w.........y...:..B.....y...... ....*Hhttps://arthurperush.com/css /cPanel.SharePoint_documentOnline/login.html2.Webmail Login:......................... ....*Whttp://v2.bpkbsaya.com/wp-includes/css/cPan

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2032
Entropy (8bit):	4.901556333062161
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDH3qyvz5sPhGsPrRLsPLPESyBsPlMHYsPYMHWbG:JTnOCXGDHa+z6V1MGwGWS
MD5:	25DE2FB0546CC1E5FD5F731E88AFB746
SHA1:	B1FE80DAAB8748B0A708137BAF3E69816687D0C8
SHA-256:	9EF8877344F28C68CB844C60CA2B7546A53115AE2907FDE7D9C0F5DC29E22ABC
SHA-512:	2E87E6683B0C82CA9DB7C98B3A15DE0446DA4B7CED97C72934CAE4A16123D915FC7B438A2EA101598E30DED49D37D32BAF83F1F3B88BD5B365482E12B3EA1: D4
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","s upports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation": [],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.c om","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://clients2.googleusercontent.com","s upports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"1330072806455183 8","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5449
Entropy (8bit):	5.000399437395531
Encrypted:	false
SSDEEP:	96:nyBCcmi1pcKI6ok0JC3RWL8NkI1hbOTQVuwn:nACK1pcD43YAkIL
MD5:	9635C218840F75F7855631A1CB2C79FD
SHA1:	33B2351AD84AC452C7345523AB337C8595FD3380
SHA-256:	16E66E72B000855C578C85F527778542014C712A807F12568559752F346A0689
SHA-512:	DDE1F4493353BC5B6BD2A0A536D967595937B1C0DE2BF365E6E4E8B1A0865CAA8E7D2AB25A5A4346F76849BE43CC3EB39D3272E24B84E43048BBA5827EF3AB 1E
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298136062885541","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19793
Entropy (8bit):	5.564410656060987
Encrypted:	false
SSDEEP:	384:MwHtkLl+AX21kXqKf/pUZNCgVLH2HfDarU/HG3ejmrH4H:WLlJ21kXqKf/pUZNCgVLH2HfGrUvG3eV
MD5:	5D1B87F0117571B08DE3AABB994FBFAC
SHA1:	DD6FC10AC64B1DC19CB84B109A47ABA603317E1C
SHA-256:	F7B08AA6CCAA7EAEA89599936B63B3325DAF763979650FA4DA122BE1FFE64AF3
SHA-512:	D16F0EE56D95C11B019F7C454FA0AAD469D13139192A5D7EB579A7326F27BEA1B7ABCD71FB1B49AFCBEA8AE7B278AD090E83CF5D3E986F644F40A1937C39E6 1A
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mh t:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihck ogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network "],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"i ncognito_content_settings":[],"incognito_preferences":{},"install_time":"13298136061753412","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome. google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons": {"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\19fa8736-0cad-4232-b7d2-b453200b1e8b.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\7e1e79ea-bcff-45de-845a-43cf18598136.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.986775197192121
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Kn:YHO8sdBsB6MAsBdLJlyH7E4f3K3X
MD5:	0D1F7A36AD610D2F08709B1EF88F1B09
SHA1:	237E8E7BC7891D987DEA1D2EB1DA9DA511396D11
SHA-256:	5C36B7E531EE8DF00FE937FDE21AF4D1B6606EAD4B5F98D56396DDCEF1C4249A
SHA-512:	37DAD8F9F2008D7B287A03964F0AE41FA4EBED92987B3872E022758857131971BC486638D0339774E80DF01A669B68DB4729D48E49EC5DE714F27ADF20B247AC
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"3G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.986775197192121
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Kn:YHO8sdBsB6MAsBdLJlyH7E4f3K3X
MD5:	0D1F7A36AD610D2F08709B1EF88F1B09
SHA1:	237E8E7BC7891D987DEA1D2EB1DA9DA511396D11
SHA-256:	5C36B7E531EE8DF00FE937FDE21AF4D1B6606EAD4B5F98D56396DDCEF1C4249A
SHA-512:	37DAD8F9F2008D7B287A03964F0AE41FA4EBED92987B3872E0227585857131971BC486638D0339774E80DF01A669B68DB4729D48E49EC5DE714F27ADF20B247AC
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"3G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\7016b328-c69b-4427-bf66-a5317616c2ba.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954409809181979
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K3X:YXsdvjX6gjXdL3yH7n/y
MD5:	F7EA7FF47D0FD3626EC4879195182336
SHA1:	B1FFD61A260C441A09C636B0F32937D08E45AE3D
SHA-256:	E52C4807EA6A80D9FE9394046D2A5CE282135C3A8C5B714F77083C907AED7C81
SHA-512:	C7D891EFDF23A367CDB27D21535D838EB44FCF98F475DAD15E9DCFB829E1F0FB0FE55B1A073548C3725A8ED5451A63405B1DE4E3726D1124AE08939B3823937 0
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"3G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE

SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954409809181979
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K3X:YXsdvjX6gjXdL3yH7n/y
MD5:	F7EA7FF47D0FD3626EC4879195182336
SHA1:	B1FFD61A260C441A09C636B0F32937D08E45AE3D
SHA-256:	E52C4807EA6A80D9FE9394046D2A5CE282135C3A8C5B714F77083C907AED7C81
SHA-512:	C7D891EFDF23A367CDB27D21535D838EB44FCF98F475DAD15E9DCFB829E1F0FB0FE55B1A073548C3725A8ED5451A63405B1DE4E3726D1124AE08939B3823937 0
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"3G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\adcadca8-7e62-4081-9b90-d2a4ceb321f6.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19792
Entropy (8bit):	5.5643571730188155
Encrypted:	false
SSDEEP:	384:MwHtkLl+AX21kXqKf/pUZNCgVLH2HfDarU/HGcej0rH4e:WLlJ21kXqKf/pUZNCgVLH2HfGrUvGce+
MD5:	6B72D0BF7D392742FC75550C34B33384
SHA1:	40177A008E67C17757B14127C3DFA389D362C7F5
SHA-256:	254394DAF39324922380CB702CCCF8550AFE74F3EB45464963867089F8FC4866
SHA-512:	FD43020C1C3A72BA886FEC24DF5707E0FE3F14CF0F7B65EEB7E220FBB5A0BA90F3CF5C999F037F12E48F1732B0196F2D6B523B2D77D7B6CBCAD35ED223FD26F0
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13298136061753412","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b4a5c365-0bc0-4e36-950a-496e402d52aa.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19793
Entropy (8bit):	5.564410656060987
Encrypted:	false
SSDEEP:	384:MwHtkLl+AX21kXqKf/pUZNCgVLH2HfDarU/HG3ejmrH4H:WLlJ21kXqKf/pUZNCgVLH2HfGrUvG3eV
MD5:	5D1B87F0117571B08DE3AABB994FBFAC
SHA1:	DD6FC10AC64B1DC19CB84B109A47ABA603317E1C
SHA-256:	F7B08AA6CCAA7EAEA89599936B63B3325DAF763979650FA4DA122BE1FFE64AF3

SHA-512:	D16F0EE56D95C11B019F7C454FA0AAD469D13139192A5D7EB579A7326F27BEA1B7ABCD71FB1B49AFCBEA8AE7B278AD090E83CF5D3E986F644F40A1937C39E6 1A
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13298136061753412","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ce47dec3-96de-4d65-8058-5b9785341d32.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5422
Entropy (8bit):	4.99609500461098
Encrypted:	false
SSDEEP:	96:nyBCcci1pcKIbok0JC3RWL8NkI1EbOTQVuwn:nACm1pc843YAkI4
MD5:	18CCB1098353A4770C3B6A113DC81E97
SHA1:	71AB878FB6665C27910473414EBFAD45BB8FAC51
SHA-256:	42184F5D8EA2A6BF3B8B4E28BF62DB20AAAD08A8B1DA0C1AF33641C2B57A9377
SHA-512:	04134E20B7475DC7A79E697E65A33F45B0AAAEBE80309CDFDAC3990485A4FF829EA243F37DE09D275AE8CBFF68D8A8D2063BDF108298A877E032ED6A31F4C3 F8
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298136062885541","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cf56e9c4-f167-4e68-9039-4911a77579ab.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5387
Entropy (8bit):	5.000145112636795
Encrypted:	false
SSDEEP:	96:nyBCcci1pcKICok0JC3RWL8NkI1EbOTQVuwn:nACm1pcP43YAkI4
MD5:	3305A763BC4D68F7FE22E6C3FDC57244
SHA1:	3CC60BB665BF455E2D50A9B414A8CC249228A342
SHA-256:	7CA5E90168F5195A64DD997AC64690DC41C425B2920A9F6988520E382FA63FD3
SHA-512:	EC959AE4EED9CF30F011BF430DC259B5975339FE6F97C7ACE4173A74775E3B20D8D219D64E733D516C94F36B42E55B97E37566AA49AD91A5A35BC29E043AD69 7
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298136062885541","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d7a0d96c-6739-4c68-badd-9b3ea09ef812.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5422
Entropy (8bit):	4.995621995473771
Encrypted:	false
SSDEEP:	96:nyBCcci1pcKI2Tok0JC3RWL8NkI1EbOTQVuwn:nACm1pckO43YAkI4
MD5:	53F7F5F65B0187A57DE9CBD5ABA25A81
SHA1:	954639D63FAD6A2C64FCBCAB092318F6BFE9B7C9
SHA-256:	76E5A45122B87F00D376CDB9F8B794B61F80FA1D5FC36BA0B3CF3D9C8FC0C9DF
SHA-512:	95A2765A5B4F423EE797C34096928077764377AA1AE5E2267484E560558F60CF5563F199F15318D5AF2F0A46213726DD028A3565D882522655E20C4CC1726E72

Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298136062885541","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWlV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWlV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\dbc05ae3-04c6-437c-9d41-b2249c7cf2c0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD160
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f73a4c12-4c3c-46cf-a067-a85e9f9e4530.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17703
Entropy (8bit):	5.57719274792536
Encrypted:	false
SSDEEP:	384:MwHtkLl+AX21kXqKf/pUZNCgVLH2HfDarUJejTrH4t:WLlJ21kXqKf/pUZNCgVLH2HfGrUJePru
MD5:	A510CA7FDF8F98940FFA70B6EEB5BE05
SHA1:	755A31ECF32514946091B89E0045CF222F334EE3
SHA-256:	3057048F3CB31D9DA6C39C6EAE1F4C7F3834EFC6D79BFE2B4633A5D8F73FE86B
SHA-512:	86C46CCA03D17A766A8560BAB9C4DA0D77E42340C1FD5070FADF247EC9F51218220AD67602435E4CB535772499176681165502B349BD544F38FA8D9DBD02538
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docxm:docm:xls:xlsx:xlsxm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz"},"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13298136061753412","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_i

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fca7bb2a-cc0f-4ec8-ac83-a7bd0567f968.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5449
Entropy (8bit):	5.000399437395531
Encrypted:	false
SSDEEP:	96:nyBCcmi1pcKI6ok0JC3RWL8NkI1hbOTQVuwn:nACK1pcD43YAkIL
MD5:	9635C218840F75F7855631A1CB2C79FD
SHA1:	33B2351AD84AC452C7345523AB337C8595FD3380
SHA-256:	16E66E72B000855C578C85F527778542014C712A807F12568559752F346A0689
SHA-512:	DDE1F4493353BC5B6BD2A0A536D967595937B1C0DE2BF365E6E4E8B1A0865CAA8E7D2AB25A5A4346F76849BE43CC3EB39D3272E24B84E43048BBA5827EF3AB 1E
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13298136062885541","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
Malicious:	false
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false

SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
Malicious:	false
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	198594
Entropy (8bit):	6.044457879375504
Encrypted:	false
SSDEEP:	6144:e7cFfKzNM+gc+VLb8eA5wc5CaqfIlUOoSiuRp:SlG9c+VLIJ515Roq
MD5:	A8961A1D4AEB2AB8ECAA02A530C36659
SHA1:	45E3EA6D99FA70EBACA0EE8B90A354D22C370B89
SHA-256:	0205760CF836E76248623FD42C9C08A8BF46B90A390B25BB47C9E8E7F3FC882E
SHA-512:	CAFD239F8333F33C2FB8E1EE5104132BFD88D7355E7E6AAC1FE6D2EDB7D38C1CA1E0170649C6787DCDE04F460F96C20E7908B11E29B1CC32F3F0352F779040A
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.653662463950412e+12,"network":1.653630064e+12,"ticks":222930665.0,"uncertainty":3243168.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639747675"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96052
Entropy (8bit):	3.746522361045131
Encrypted:	false
SSDEEP:	384:hTfE0W5jytuIVxDg7N8rdv40330SbHmzGzWrRmcGxOUqaqtrpMm9xr1WE4o7O2ai:NWylJyQQH8evqAi0vfuIKmgQhb
MD5:	79BCBAB582F0670623795488A0D8246D
SHA1:	642E48422368EC7DFD02EF41E7B09E06CCEC1916
SHA-256:	FE0FA9BB0691AED0858083CFB5B836727A582DB523B94412D5CB617BD91BF74C
SHA-512:	C3056A955896AFFF6D345422B6E71061C98FA797C14AF01927898A2005E83661FECDB8B030BC02D95CB5EBD2BF4F525BCD7E6AD59EA713EC78021850F7EF1390
Malicious:	false
Preview:	0w.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{}...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...f]8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\a96e33c5-d810-4ba1-8939-5076c58bd766.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	206868
Entropy (8bit):	6.072455948695526
Encrypted:	false
SSDEEP:	6144:Qf7cFfKzNM+gc+VLb8eA5wc5CaqfIlUOoSiuRp:QDlG9c+VLIJ515Roq
MD5:	10A2471ADCA2B573B53D7055DFB08F45
SHA1:	0FF60A738AD3838EE947D09388A251F1AFF8A872
SHA-256:	F8D0C34521BCFD14FA2D8F236BA8BCD919CD961F5BC038CB0EE60056D066010E
SHA-512:	FE3A2EF6851FD708305883897D853A6C30ABDBD6EA9198EF7464521C9E783C9C535881BC26B59C4471C2A91C00D25F51478917353A6C43FBB63A105CD2645BD

Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.653662463950412e+12,"network":1.653630064e+12,"ticks":222930665.0,"uncertainty":3243168.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639747675"},"plugins":{"metadata":{"adobe-flash-player":{"disp

Static File Info

General

File type:	PDF document, version 1.7
Entropy (8bit):	7.613641116238123
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	View Shared File.pdf
File size:	52773
MD5:	0a2fecc6ab069dd0c654b702b8f4d3fd
SHA1:	7f1092ab0289b76ab0f1c30deacbfa67a656253e
SHA256:	4fab88614d666873895c79011f4aa5c7642bf3ba91f5b0a8fe67b059e676767e
SHA512:	f5ac1fe4dbc8c005b3084048b4da6fe8a4bd5259672dc2c958e8b32c7a7957abbf0938337158e1615cd9edb71ee301c6b149c1e85fca16000947ec90577943fa
SSDEEP:	1536:011ARZgvSIof2ikKoeqDQdQC1qS+199f9:PuvSIGhJdQ+qS899F
TLSH:	EF33E084D0BC15A5D83C94B2B7228C57F0E5D1ADC4AAB9D8356DC0C71686EA772C3E8F
File Content Preview:	%PDF-1.7..%.....1 0 obj..<</Pages 2 0 R /Type/Catalog>>..endobj..3 0 obj..<</ColorSpace/DeviceRGB/Length 47552/BitsPerComponent 8/Width 1600/Height 1600/Filter/FlateDecode/Subtype/Image/Type/XObject>>stream..x.....%.}..B.....9..'...zf..<.l..<cz..5....<

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

Header:	%PDF-1.7
Total Entropy:	7.613641
Total Bytes:	52773
Stream Entropy:	7.582999
Stream Bytes:	49373
Entropy outside Streams:	0.000000
Bytes outside Streams:	3400
Number of EOF found:	1
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	18
endobj	18
stream	15
endstream	15
xref	0
trailer	0
startxref	1
/Page	1
/Encrypt	0
/ObjStm	1
/URI	0
/JS	0
/JavaScript	0

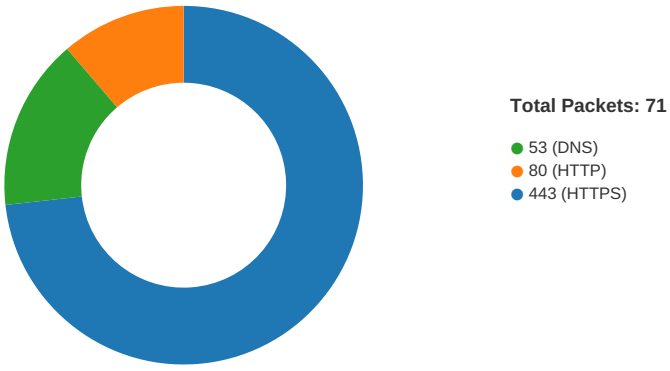
Name	Count
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Image Streams

ID	DHASH	MD5	Preview
3	49f0e0f20c200000	01c2364385bd0eec1b763c6a54b6d19f	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 07:41:03.879125118 CEST	49809	443	192.168.2.3	142.250.203.109
May 27, 2022 07:41:03.879192114 CEST	443	49809	142.250.203.109	192.168.2.3
May 27, 2022 07:41:03.879334927 CEST	49809	443	192.168.2.3	142.250.203.109
May 27, 2022 07:41:03.879815102 CEST	49809	443	192.168.2.3	142.250.203.109
May 27, 2022 07:41:03.879843950 CEST	443	49809	142.250.203.109	192.168.2.3
May 27, 2022 07:41:03.880563974 CEST	49810	80	192.168.2.3	203.161.184.43
May 27, 2022 07:41:03.881279945 CEST	49811	80	192.168.2.3	203.161.184.43
May 27, 2022 07:41:03.884318113 CEST	49812	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:03.884350061 CEST	443	49812	216.58.215.238	192.168.2.3
May 27, 2022 07:41:03.884458065 CEST	49812	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:03.884680033 CEST	49812	443	192.168.2.3	216.58.215.238

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 07:41:03.884705067 CEST	443	49812	216.58.215.238	192.168.2.3
May 27, 2022 07:41:03.934380054 CEST	443	49809	142.250.203.109	192.168.2.3
May 27, 2022 07:41:03.934838057 CEST	49809	443	192.168.2.3	142.250.203.109
May 27, 2022 07:41:03.934900045 CEST	443	49809	142.250.203.109	192.168.2.3
May 27, 2022 07:41:03.936014891 CEST	443	49809	142.250.203.109	192.168.2.3
May 27, 2022 07:41:03.936192989 CEST	49809	443	192.168.2.3	142.250.203.109
May 27, 2022 07:41:03.946211100 CEST	443	49812	216.58.215.238	192.168.2.3
May 27, 2022 07:41:03.949117899 CEST	49812	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:03.949147940 CEST	443	49812	216.58.215.238	192.168.2.3
May 27, 2022 07:41:03.949485064 CEST	443	49812	216.58.215.238	192.168.2.3
May 27, 2022 07:41:03.949568033 CEST	49812	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:03.950318098 CEST	443	49812	216.58.215.238	192.168.2.3
May 27, 2022 07:41:03.950417042 CEST	49812	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:04.086373091 CEST	49813	80	192.168.2.3	203.161.184.43
May 27, 2022 07:41:04.089272976 CEST	80	49811	203.161.184.43	192.168.2.3
May 27, 2022 07:41:04.089390039 CEST	49811	80	192.168.2.3	203.161.184.43
May 27, 2022 07:41:04.089963913 CEST	49811	80	192.168.2.3	203.161.184.43
May 27, 2022 07:41:04.090914965 CEST	80	49810	203.161.184.43	192.168.2.3
May 27, 2022 07:41:04.091074944 CEST	49810	80	192.168.2.3	203.161.184.43
May 27, 2022 07:41:04.224097967 CEST	49812	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:04.224291086 CEST	49809	443	192.168.2.3	142.250.203.109
May 27, 2022 07:41:04.224356890 CEST	443	49812	216.58.215.238	192.168.2.3
May 27, 2022 07:41:04.224647045 CEST	49812	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:04.224668026 CEST	443	49812	216.58.215.238	192.168.2.3
May 27, 2022 07:41:04.224714994 CEST	443	49809	142.250.203.109	192.168.2.3
May 27, 2022 07:41:04.224855900 CEST	49809	443	192.168.2.3	142.250.203.109
May 27, 2022 07:41:04.224903107 CEST	443	49809	142.250.203.109	192.168.2.3
May 27, 2022 07:41:04.258543968 CEST	443	49812	216.58.215.238	192.168.2.3
May 27, 2022 07:41:04.258625984 CEST	49812	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:04.258647919 CEST	443	49812	216.58.215.238	192.168.2.3
May 27, 2022 07:41:04.258685112 CEST	443	49812	216.58.215.238	192.168.2.3
May 27, 2022 07:41:04.258744001 CEST	49812	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:04.265600920 CEST	49809	443	192.168.2.3	142.250.203.109
May 27, 2022 07:41:04.267152071 CEST	49812	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:04.267183065 CEST	443	49812	216.58.215.238	192.168.2.3
May 27, 2022 07:41:04.278213978 CEST	443	49809	142.250.203.109	192.168.2.3
May 27, 2022 07:41:04.278347969 CEST	49809	443	192.168.2.3	142.250.203.109
May 27, 2022 07:41:04.278414011 CEST	443	49809	142.250.203.109	192.168.2.3
May 27, 2022 07:41:04.278588057 CEST	443	49809	142.250.203.109	192.168.2.3
May 27, 2022 07:41:04.278660059 CEST	49809	443	192.168.2.3	142.250.203.109
May 27, 2022 07:41:04.288234949 CEST	49809	443	192.168.2.3	142.250.203.109
May 27, 2022 07:41:04.288279057 CEST	443	49809	142.250.203.109	192.168.2.3
May 27, 2022 07:41:04.290319920 CEST	80	49813	203.161.184.43	192.168.2.3
May 27, 2022 07:41:04.290488958 CEST	49813	80	192.168.2.3	203.161.184.43
May 27, 2022 07:41:04.299093962 CEST	80	49811	203.161.184.43	192.168.2.3
May 27, 2022 07:41:04.316817999 CEST	80	49811	203.161.184.43	192.168.2.3
May 27, 2022 07:41:04.358309984 CEST	49811	80	192.168.2.3	203.161.184.43
May 27, 2022 07:41:05.026315928 CEST	49818	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.026376963 CEST	443	49818	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.026484013 CEST	49818	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.027105093 CEST	49819	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.027156115 CEST	443	49819	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.027240992 CEST	49819	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.027333975 CEST	49818	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.027368069 CEST	443	49818	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.027947903 CEST	49819	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.027976036 CEST	443	49819	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.419115067 CEST	443	49819	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.419147015 CEST	443	49818	138.59.135.12	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 07:41:05.466413975 CEST	49819	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.508562088 CEST	49818	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.569785118 CEST	49818	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.569825888 CEST	443	49818	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.569928885 CEST	49819	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.569956064 CEST	443	49819	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.572207928 CEST	443	49819	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.572319031 CEST	49819	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.572343111 CEST	443	49819	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.572923899 CEST	443	49818	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.572988033 CEST	443	49818	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.573012114 CEST	49818	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.576775074 CEST	49819	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.576983929 CEST	443	49819	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.577070951 CEST	49818	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.577393055 CEST	443	49818	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.577956915 CEST	49819	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.577976942 CEST	443	49819	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.622477055 CEST	49819	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.708482981 CEST	49818	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.708523989 CEST	443	49818	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.784564018 CEST	443	49819	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.784609079 CEST	443	49819	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.784624100 CEST	443	49819	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.784681082 CEST	443	49819	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.784688950 CEST	49819	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.784723997 CEST	443	49819	138.59.135.12	192.168.2.3
May 27, 2022 07:41:05.784739971 CEST	49819	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.784746885 CEST	49819	443	192.168.2.3	138.59.135.12
May 27, 2022 07:41:05.808459044 CEST	49818	443	192.168.2.3	138.59.135.12

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 07:40:48.298374891 CEST	53802	53	192.168.2.3	8.8.8.8
May 27, 2022 07:40:48.631707907 CEST	53	53802	8.8.8.8	192.168.2.3
May 27, 2022 07:41:03.845320940 CEST	50152	53	192.168.2.3	8.8.8.8
May 27, 2022 07:41:03.846471071 CEST	56639	53	192.168.2.3	8.8.8.8
May 27, 2022 07:41:03.848342896 CEST	50450	53	192.168.2.3	8.8.8.8
May 27, 2022 07:41:03.865741968 CEST	53	56639	8.8.8.8	192.168.2.3
May 27, 2022 07:41:03.875458956 CEST	53	50450	8.8.8.8	192.168.2.3
May 27, 2022 07:41:03.883115053 CEST	53	50152	8.8.8.8	192.168.2.3
May 27, 2022 07:41:04.668555021 CEST	54960	53	192.168.2.3	8.8.8.8
May 27, 2022 07:41:05.024938107 CEST	53	54960	8.8.8.8	192.168.2.3
May 27, 2022 07:41:06.091727972 CEST	64624	53	192.168.2.3	8.8.8.8
May 27, 2022 07:41:06.111586094 CEST	53	64624	8.8.8.8	192.168.2.3
May 27, 2022 07:41:08.957313061 CEST	62701	53	192.168.2.3	8.8.8.8
May 27, 2022 07:41:08.976121902 CEST	53	62701	8.8.8.8	192.168.2.3
May 27, 2022 07:41:09.687304020 CEST	53524	53	192.168.2.3	8.8.8.8
May 27, 2022 07:41:09.704642057 CEST	53	53524	8.8.8.8	192.168.2.3
May 27, 2022 07:41:09.835326910 CEST	58561	53	192.168.2.3	8.8.8.8
May 27, 2022 07:41:09.978439093 CEST	53	58561	8.8.8.8	192.168.2.3
May 27, 2022 07:41:10.585745096 CEST	58562	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:10.616600990 CEST	443	58562	216.58.215.238	192.168.2.3
May 27, 2022 07:41:10.617039919 CEST	58562	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:10.647806883 CEST	443	58562	216.58.215.238	192.168.2.3
May 27, 2022 07:41:10.647830963 CEST	443	58562	216.58.215.238	192.168.2.3
May 27, 2022 07:41:10.647845984 CEST	443	58562	216.58.215.238	192.168.2.3
May 27, 2022 07:41:10.647862911 CEST	443	58562	216.58.215.238	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 07:41:10.655071020 CEST	58562	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:10.656688929 CEST	58562	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:10.688718081 CEST	58562	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:10.689308882 CEST	58562	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:10.729998112 CEST	443	58562	216.58.215.238	192.168.2.3
May 27, 2022 07:41:10.730669975 CEST	58562	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:10.732239962 CEST	443	58562	216.58.215.238	192.168.2.3
May 27, 2022 07:41:10.746449947 CEST	443	58562	216.58.215.238	192.168.2.3
May 27, 2022 07:41:10.746484995 CEST	443	58562	216.58.215.238	192.168.2.3
May 27, 2022 07:41:10.746505976 CEST	443	58562	216.58.215.238	192.168.2.3
May 27, 2022 07:41:10.747826099 CEST	58562	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:10.776433945 CEST	58562	443	192.168.2.3	216.58.215.238
May 27, 2022 07:41:12.201355934 CEST	62547	53	192.168.2.3	8.8.8.8
May 27, 2022 07:41:12.338187933 CEST	53	62547	8.8.8.8	192.168.2.3
May 27, 2022 07:41:18.373362064 CEST	57829	53	192.168.2.3	8.8.8.8
May 27, 2022 07:41:18.694408894 CEST	53	57829	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 07:40:48.298374891 CEST	192.168.2.3	8.8.8.8	0xf71e	Standard query (0)	bpkbsaya.com	A (IP address)	IN (0x0001)
May 27, 2022 07:41:03.845320940 CEST	192.168.2.3	8.8.8.8	0x7c5	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
May 27, 2022 07:41:03.846471071 CEST	192.168.2.3	8.8.8.8	0x6877	Standard query (0)	v2.bpkbsaya.com	A (IP address)	IN (0x0001)
May 27, 2022 07:41:03.848342896 CEST	192.168.2.3	8.8.8.8	0xbc7	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
May 27, 2022 07:41:04.668555021 CEST	192.168.2.3	8.8.8.8	0xfe65	Standard query (0)	arthurperush.com	A (IP address)	IN (0x0001)
May 27, 2022 07:41:06.091727972 CEST	192.168.2.3	8.8.8.8	0x769d	Standard query (0)	webmail.unitedyacht.com	A (IP address)	IN (0x0001)
May 27, 2022 07:41:08.957313061 CEST	192.168.2.3	8.8.8.8	0x9b99	Standard query (0)	i.imgur.com	A (IP address)	IN (0x0001)
May 27, 2022 07:41:09.687304020 CEST	192.168.2.3	8.8.8.8	0x1a24	Standard query (0)	i.imgur.com	A (IP address)	IN (0x0001)
May 27, 2022 07:41:09.835326910 CEST	192.168.2.3	8.8.8.8	0xafb7	Standard query (0)	webmail.unitedyacht.com	A (IP address)	IN (0x0001)
May 27, 2022 07:41:12.201355934 CEST	192.168.2.3	8.8.8.8	0x9993	Standard query (0)	webmail.serendahsteel.com	A (IP address)	IN (0x0001)
May 27, 2022 07:41:18.373362064 CEST	192.168.2.3	8.8.8.8	0x35c4	Standard query (0)	webmail.serendahsteel.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 07:40:48.631707907 CEST	8.8.8.8	192.168.2.3	0xf71e	No error (0)	bpkbsaya.com		203.161.184.43	A (IP address)	IN (0x0001)
May 27, 2022 07:41:03.865741968 CEST	8.8.8.8	192.168.2.3	0x6877	No error (0)	v2.bpkbsaya.com		203.161.184.43	A (IP address)	IN (0x0001)
May 27, 2022 07:41:03.875458956 CEST	8.8.8.8	192.168.2.3	0xbc7	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)
May 27, 2022 07:41:03.883115053 CEST	8.8.8.8	192.168.2.3	0x7c5	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 07:41:03.883115053 CEST	8.8.8.8	192.168.2.3	0x7c5	No error (0)	clients.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
May 27, 2022 07:41:05.024938107 CEST	8.8.8.8	192.168.2.3	0xfe65	No error (0)	arthurperush.com		138.59.135.12	A (IP address)	IN (0x0001)
May 27, 2022 07:41:06.111586094 CEST	8.8.8.8	192.168.2.3	0x769d	No error (0)	webmail.unitedyacht.com		72.9.144.117	A (IP address)	IN (0x0001)
May 27, 2022 07:41:08.976121902 CEST	8.8.8.8	192.168.2.3	0x9b99	No error (0)	i.imgur.com	ipv4.imgur.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 07:41:08.976121902 CEST	8.8.8.8	192.168.2.3	0x9b99	No error (0)	ipv4.imgur.map.fastly.net		151.101.112.193	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 07:41:09.704642057 CEST	8.8.8.8	192.168.2.3	0x1a24	No error (0)	i.imgur.com	ipv4.imgur.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 07:41:09.704642057 CEST	8.8.8.8	192.168.2.3	0x1a24	No error (0)	ipv4.imgur.map.fastly.net		151.101.112.193	A (IP address)	IN (0x0001)
May 27, 2022 07:41:09.978439093 CEST	8.8.8.8	192.168.2.3	0xafb7	No error (0)	webmail.unitedyacht.com		72.9.144.117	A (IP address)	IN (0x0001)
May 27, 2022 07:41:12.338187933 CEST	8.8.8.8	192.168.2.3	0x9993	No error (0)	webmail.serendahsteel.com		103.6.196.136	A (IP address)	IN (0x0001)
May 27, 2022 07:41:12.338187933 CEST	8.8.8.8	192.168.2.3	0x9993	No error (0)	webmail.serendahsteel.com		110.4.45.141	A (IP address)	IN (0x0001)
May 27, 2022 07:41:18.694408894 CEST	8.8.8.8	192.168.2.3	0x35c4	No error (0)	webmail.serendahsteel.com		110.4.45.141	A (IP address)	IN (0x0001)
May 27, 2022 07:41:18.694408894 CEST	8.8.8.8	192.168.2.3	0x35c4	No error (0)	webmail.serendahsteel.com		103.6.196.136	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- v2.bpkbsaya.com
  - arthurperush.com
- https:
  - webmail.unitedyacht.com
  - i.imgur.com
  - webmail.serendahsteel.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49812	216.58.215.238	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49809	142.250.203.109	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49833	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49834	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49837	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49838	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49839	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49841	151.101.112.193	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49846	151.101.112.193	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49849	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49848	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49851	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49819	138.59.135.12	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49850	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49852	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49856	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49857	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49859	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49860	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49862	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49861	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49863	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49864	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49825	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49865	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49866	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49872	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49871	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49873	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49884	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49885	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49902	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49933	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49946	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49824	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49956	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49966	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49975	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	50003	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	50011	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	50019	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.3	50026	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.3	50033	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	50038	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	50044	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49828	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.3	49811	203.161.184.43	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 07:41:04.089963913 CEST	8498	OUT	GET /wp-includes/css/cPanel.SharePoint_documentOnline/redirecting.php HTTP/1.1 Host: v2.bpkbsaya.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
May 27, 2022 07:41:04.316817999 CEST	8544	IN	HTTP/1.1 200 OK Connection: Keep-Alive X-Powered-By: PHP/7.2.34 Content-Type: text/html; charset=UTF-8 Content-Length: 134 Content-Encoding: gzip Vary: Accept-Encoding Date: Fri, 27 May 2022 05:41:04 GMT Server: LiteSpeed X-Powered-By: PleskLin Data Raw: 1f 8b 08 00 00 00 00 00 03 2d cd 31 0e c2 30 0c 00 c0 bd 52 fe c0 d6 2d d9 a1 45 fc 80 4a 3c a0 b2 5c 2b 31 4a ec 28 71 e8 f7 19 60 bd e5 96 8e 8d ab 5d 32 48 1c 10 69 7d c3 07 7e 76 77 93 9b 4e 96 43 4f 9f 15 c1 58 65 9d 93 59 ed d7 10 1e d0 2c 8d 56 a9 8d 9e 3c 6a 09 d8 7b c0 0d 84 b2 7f 25 68 b4 29 8b ed 87 e2 28 24 f6 94 cc 42 21 6b 64 f1 c9 4a 9e 6f 6e 5a c2 bf fa 02 21 32 42 c3 87 00 00 00 Data Ascii: -10R-EJ<\+1J(q`]2Hi}~vwNCOXeY,V<j{%h)($B!kdJonZ!2B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49829	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49830	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49832	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49831	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49812	216.58.215.238	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:04 UTC	0	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda,pkedcjkdefgpdelpbcmbmeomcjbeemfm X-Goog-Update-Updater: chromecrx-85.0.4183.121 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 05:41:04 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-8iCvXEGWkPp_csgrykH3hg' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 05:41:04 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5624 X-Daystart: 81664 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 05:41:04 UTC	2	IN	Data Raw: 33 36 64 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 36 32 34 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 38 31 36 36 34 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 Data Ascii: 36d<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" protocol="2.0" server="prod"><daystart elapsed_days="5624" elapsed_seconds="81664"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""
2022-05-27 05:41:04 UTC	2	IN	Data Raw: 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 70 Data Ascii: mhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><ap
2022-05-27 05:41:04 UTC	3	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49809	142.250.203.109	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:04 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 05:41:04 UTC	1	OUT	Data Raw: 20 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:04 UTC	3	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 05:41:04 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-33GWpkHDIeJuG-WJcVFTFw' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-33GWpkHDIeJuG-WJcVFTFw' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Cross-Origin-Opener-Policy: same-origin Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 05:41:04 UTC	4	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]
2022-05-27 05:41:04 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49833	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:07 UTC	200	OUT	GET /cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Semibold-webfont.woff HTTP/1.1 Host: webmail.unitedyacht.com Connection: keep-alive Origin: https://arthurperush.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: font Referer: https://webmail.unitedyacht.com/cPanel_magic_revision_1386192030/unprotected/cpanel/fonts/open_sans/open_sans.min.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 05:41:08 UTC	211	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:08 GMT Server: Apache/2.4.53 (cPanel) OpenSSL/1.1.1o mod_bwlimited/1.4 Content-Type: application/font-woff Last-Modified: Tue, 23 Mar 2021 16:37:21 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:08 GMT Content-Length: 22908 Vary: Accept-Encoding,User-Agent Connection: close
2022-05-27 05:41:08 UTC	211	IN	Data Raw: 77 4f 46 46 00 01 00 00 00 00 59 7c 00 13 00 00 00 00 9a 34 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 46 46 54 4d 00 00 01 a8 00 00 00 1c 00 00 00 1c 63 5f a5 d6 47 44 45 46 00 00 01 c4 00 00 00 1e 00 00 00 20 01 1c 00 04 47 50 4f 53 00 00 01 e4 00 00 04 a3 00 00 09 9e 2d 72 17 42 47 53 55 42 00 00 06 88 00 00 00 81 00 00 00 a8 a0 62 88 9e 4f 53 2f 32 00 00 07 0c 00 00 00 5f 00 00 00 60 a1 cc 92 87 63 6d 61 70 00 00 07 6c 00 00 01 9c 00 00 02 02 b7 6f 6c be 63 76 74 20 00 00 09 08 00 00 00 30 00 00 00 3c 2a 72 06 89 66 70 67 6d 00 00 09 38 00 00 04 fa 00 00 09 91 8b 0b 7a 41 67 61 73 70 00 00 0e 34 00 00 00 08 00 00 00 08 00 00 00 10 67 6c 79 66 00 00 0e 3c 00 00 42 2a 00 00 73 e8 80 99 2f ad 68 65 61 64 00 00 50 68 00 00 00 Data Ascii: wOFFY|4FFTMc_GDEF GPOS-rBGSUBbOS/2_`cmaplolcvt 0<*rfpgm8zAgasp4glyf<B*s/headPh

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:08 UTC	219	IN	Data Raw: 31 09 c6 f8 2e f7 0a d2 a6 0e d7 b7 89 98 5e 16 c1 47 35 cf 7a 95 b6 da 78 5c d6 69 08 0c 78 dd d1 c6 ba e9 14 29 af d4 b1 53 4d 5d 4d 4a c4 49 54 19 47 55 6a 3d 25 2f e9 b3 67 5d 93 09 97 9b e9 06 4f 29 65 28 ff 9c ef 4f fc a7 f1 2e f1 e8 bc 9d 42 42 e3 5d e5 04 5b cf 5e 61 2f b3 27 d1 20 0c 82 7e 30 f1 f2 a6 4f 3e fa f0 e4 c7 1f 7e 7c 8a 9e c6 cf ee 45 ce ae c1 3f 73 d9 74 b6 8e 9d 67 df 80 13 6c 48 ba 68 f6 2d 31 74 90 bc 50 c4 bd 0e 43 92 91 b5 08 0f 09 85 ac 05 43 ad b4 54 8f 2d 55 a4 37 65 8f 08 b3 52 e4 e6 40 50 5e c8 fe ce ce ad f9 01 9e 01 3b d8 9a 32 66 ef 7e 7e dd d3 9b a5 c6 33 17 38 5b fc 93 45 3f fc c8 43 0f f2 b5 66 b2 4d 02 df 48 f4 35 da 07 32 70 0b 25 1e 05 00 b9 33 b8 9c f0 4b 9a dd c6 b4 34 8f 48 a9 46 f1 74 58 50 b6 db e2 ff ee 41 18 Data Ascii: 1.^G5zx\ix)SM]MJITGUj=%/g]O)e(O.BB][^a/' ~0O>~|E?stglHh-1tPCCT-U7eR@P^;2f~~38[E?CfMH52p% 3K4HFtXPA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49834	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:07 UTC	200	OUT	GET /cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Bold-webfont.woff HTTP/1.1 Host: webmail.unitedyacht.com Connection: keep-alive Origin: https://arthurperush.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183. 121 Safari/537.36 Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: font Referer: https://webmail.unitedyacht.com/cPanel_magic_revision_1386192030/unprotected/cpanel/fonts/open_sans/o pen_sans.min.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 05:41:08 UTC	219	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:08 GMT Server: Apache/2.4.53 (cPanel) OpenSSL/1.1.1o mod_bwlimited/1.4 Content-Type: application/font-woff Last-Modified: Tue, 23 Mar 2021 16:37:21 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:08 GMT Content-Length: 22432 Vary: Accept-Encoding,User-Agent Connection: close
2022-05-27 05:41:08 UTC	219	IN	Data Raw: 77 4f 46 46 00 01 00 00 00 00 57 a0 00 13 00 00 00 00 96 34 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 46 46 54 4d 00 00 01 a8 00 00 00 1c 00 00 00 1c 63 54 d3 4e 47 44 45 46 00 00 01 c4 00 00 00 1e 00 00 00 20 01 1c 00 04 47 50 4f 53 00 00 01 e4 00 00 04 a3 00 00 09 9e 2d 72 17 42 47 53 55 42 00 00 06 88 00 00 00 81 00 00 00 a8 a0 62 88 9e 4f 53 2f 32 00 00 07 0c 00 00 00 60 00 00 00 60 a2 49 9b dd 63 6d 61 70 00 00 07 6c 00 00 01 9c 00 00 02 02 b7 6f 6c be 63 76 74 20 00 00 09 08 00 00 00 32 00 00 00 3c 2b 73 06 e0 66 70 67 6d 00 00 09 3c 00 00 04 fa 00 00 09 91 8b 0b 7a 41 67 61 73 70 00 00 0e 38 00 00 00 08 00 00 00 08 00 00 00 10 67 6c 79 66 00 00 0e 40 00 00 40 76 00 00 70 58 80 78 59 fa 68 65 61 64 00 00 4e b8 00 00 00 Data Ascii: wOFFW4FFTMcTNGDEF GPOS-rBGSUBbOS/2``lcmaplolcvt 2<+sfpgm<zAgasp8glyf@@vpXxYheadN
2022-05-27 05:41:08 UTC	227	IN	Data Raw: f8 67 e2 a5 0f 5e 7d 05 66 b1 e5 af ec a6 27 d8 4a 36 0f 1e 80 69 f8 67 21 ea 8e 27 be bb 00 5f c3 d9 1f db 74 91 bc 59 e8 22 87 d8 d1 f8 99 a4 27 01 85 69 17 3a 29 46 2a f3 d8 bc be 74 9e ca 8c a8 64 05 43 39 11 28 a5 cb 70 76 d2 f2 47 e6 2c 58 46 77 b3 0f d9 37 8b 51 2e 8e 62 70 ec 92 d4 99 53 a7 35 be 7d e6 62 eb 05 65 e7 29 41 27 9a 0d 4e 67 2c fa 09 5d 43 01 5c 3e 89 7b ef 40 a6 20 a6 f6 c8 36 b2 c5 91 64 8f 48 9f c6 51 0d c5 ce 7b 35 ba 5f 7e 11 c6 b1 59 ec bc fb 9a c4 33 f6 5c 25 9b 03 83 af ca 01 5d 17 0f 16 f4 bb b9 ad 74 f0 b4 0f ce 09 8d 16 e5 aa 27 9c a6 6c cb 4a 1b 8d 46 b7 d1 ed f6 d8 7d dc 60 45 19 28 c1 09 6e bc 88 db 03 70 b6 e1 f1 87 97 af aa 47 56 6c 86 ae d0 e5 91 fb a0 bc 81 6d 62 cf 49 b9 e3 27 37 8e 69 9d db 7a 58 d9 f9 e1 89 85 87 Data Ascii: g^}f'J6ig!'_tY'"i:)F*tdC9(pvG,XFw7Q.bpS5}be)A'Ng,]C\>{@ 6dHQ{5_~Y3\%]t'lJF}`E(npGVlmbI'7izX

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49837	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:08 UTC	237	OUT	GET /cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Regular-webfont.ttf HTTP/1.1 Host: webmail.unitedyacht.com Connection: keep-alive Origin: https://arthurperush.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: font Referer: https://webmail.unitedyacht.com/cPanel_magic_revision_1386192030/unprotected/cpanel/fonts/open_sans/open_sans.min.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 05:41:08 UTC	239	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:08 GMT Server: Apache/2.4.53 (cPanel) OpenSSL/1.1.1o mod_bwlimited/1.4 Content-Type: application/octet-stream Last-Modified: Tue, 23 Mar 2021 16:37:21 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:08 GMT Content-Length: 38232 Vary: Accept-Encoding,User-Agent Connection: close
2022-05-27 05:41:08 UTC	239	IN	Data Raw: 00 01 00 00 00 13 01 00 00 04 00 30 46 46 54 4d 63 47 ec 8f 00 00 01 3c 00 00 00 1c 47 44 45 46 01 1d 00 04 00 00 01 58 00 00 00 20 47 50 4f 53 2d 72 17 42 00 00 01 78 00 00 09 9e 47 53 55 42 a0 63 88 a1 00 00 0b 18 00 00 00 a8 4f 53 2f 32 a0 e5 99 7f 00 00 0b c0 00 00 00 60 63 6d 61 70 13 f0 34 51 00 00 0c 20 00 00 02 0a 63 76 74 20 29 c6 06 3b 00 00 0e 2c 00 00 00 3c 66 70 67 6d 8b 0b 7a 41 00 00 0e 68 00 00 09 91 67 61 73 70 00 00 00 10 00 00 17 fc 00 00 00 08 67 6c 79 66 52 6a bc 2d 00 00 18 04 00 00 6f 70 68 65 61 64 01 04 94 82 00 00 87 74 00 00 00 36 68 68 65 61 0e 8c 05 19 00 00 87 ac 00 00 00 24 68 6d 74 78 fd 8b 59 db 00 00 87 d0 00 00 03 c0 6c 6f 63 61 ba 55 9f 66 00 00 8b 90 00 00 01 e2 6d 61 78 70 03 1b 02 07 00 00 8d 74 00 00 00 20 6e 61 6d Data Ascii: 0FFTMcG<GDEFX GPOS-rBxGSUBcOS/2`cmap4Q cvt);,<fpgmzAhgaspglyfRj-opheadt6hhea$hmtxYlocaU fmaxpt nam
2022-05-27 05:41:08 UTC	247	IN	Data Raw: 00 02 05 02 45 11 11 11 11 11 10 06 15 2b 01 21 15 21 11 23 11 21 35 21 11 33 02 8d 01 9c fe 64 8b fe 66 01 9a 8b 03 17 8a fe 56 01 aa 8a 01 ac 00 00 00 00 01 00 3f fe f8 01 6d 00 ee 00 08 00 24 40 21 01 01 00 01 01 42 02 01 01 00 00 01 4d 02 01 01 01 00 51 00 00 01 00 45 00 00 00 08 00 08 14 03 10 2b 25 17 06 02 07 23 36 12 37 01 5e 0f 1a 62 35 7d 1b 41 0d ee 17 64 fe f7 72 68 01 32 5c 00 00 01 00 54 01 d9 02 3f 02 71 00 03 00 1d 40 1a 00 00 01 01 00 4d 00 00 00 01 51 02 01 01 00 01 45 00 00 00 03 00 03 11 03 10 2b 13 35 21 15 54 01 eb 01 d9 98 98 00 00 00 01 00 98 ff e3 01 89 00 f2 00 0b 00 12 40 0f 00 00 00 01 53 00 01 01 15 01 44 24 22 02 11 2b 37 34 36 33 32 16 15 14 06 23 22 26 98 3d 39 3a 41 42 39 33 43 6a 43 45 45 43 41 46 3f 00 00 00 00 01 00 14 Data Ascii: E+!!#!5!3dfV?m$@!BMQE+%#67^b5}Adrh2\T?q@MQE+5!T@SD$"+74632#"&=9:AB93CjCEECAF?

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49838	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:08 UTC	238	OUT	GET /cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Semibold-webfont.ttf HTTP/1.1 Host: webmail.unitedyacht.com Connection: keep-alive Origin: https://arthurperush.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: font Referer: https://webmail.unitedyacht.com/cPanel_magic_revision_1386192030/unprotected/cpanel/fonts/open_sans/open_sans.min.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 05:41:08 UTC	248	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:08 GMT Server: Apache/2.4.53 (cPanel) OpenSSL/1.1.1o mod_bwlimited/1.4 Content-Type: application/octet-stream Last-Modified: Tue, 23 Mar 2021 16:37:21 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:08 GMT Content-Length: 39476 Vary: Accept-Encoding,User-Agent Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:08 UTC	248	IN	Data Raw: 00 01 00 00 00 13 01 00 00 04 00 30 46 46 54 4d 63 5f a5 d6 00 00 01 3c 00 00 00 1c 47 44 45 46 01 1c 00 04 00 00 01 58 00 00 00 20 47 50 4f 53 2d 72 17 42 00 00 01 78 00 00 09 9e 47 53 55 42 a0 62 88 9e 00 00 0b 18 00 00 00 a8 4f 53 2f 32 a1 cc 92 87 00 00 0b c0 00 00 00 60 63 6d 61 70 b7 6f 6c be 00 00 0c 20 00 00 02 02 63 76 74 20 2a 72 06 89 00 00 0e 24 00 00 00 3c 66 70 67 6d 8b 0b 7a 41 00 00 0e 60 00 00 09 91 67 61 73 70 00 00 00 10 00 00 17 f4 00 00 00 08 67 6c 79 66 80 99 2f ad 00 00 17 fc 00 00 73 e8 68 65 61 64 01 03 95 30 00 00 8b e4 00 00 00 36 68 68 65 61 0e 8 c 05 0b 00 00 8c 1c 00 00 00 24 68 6d 74 78 14 c8 52 d5 00 00 8c 40 00 00 03 bc 6c 6f 63 61 b0 55 ce 62 00 00 8f fc 00 0 0 01 e0 6d 61 78 70 03 1a 02 01 00 00 91 dc 00 00 00 20 6e 61 6d Data Ascii: 0FFTMc_<GDEFX GPOS-rBxGSUBbOS/2`cmapol cvt *r$<fpgmzA`gaspglyf/shead06hhea$hmtxR@locaUbm axp nam
2022-05-27 05:41:08 UTC	263	IN	Data Raw: c1 02 4a 02 89 00 03 00 1d 40 1a 00 00 01 01 00 4d 00 00 00 01 51 02 01 01 00 01 45 00 00 00 03 00 03 11 03 10 2b 13 35 21 15 48 02 02 01 c1 c8 c8 00 00 00 01 00 85 ff e3 01 ae 01 14 00 0b 00 12 40 0f 00 00 00 01 53 00 01 01 15 01 44 24 22 02 11 2b 37 34 36 33 32 16 15 14 06 23 22 26 85 4c 48 49 4c 4d 48 48 4c 7d 49 4e 51 46 47 53 52 00 00 00 00 01 00 10 00 00 03 0e 05 b6 00 03 00 18 40 15 02 01 01 01 0c 43 00 00 00 0d 00 44 00 00 00 03 00 03 11 03 10 2b 09 01 23 01 03 0e fd e0 de 02 21 05 b6 fa 4a 05 b6 00 00 02 00 58 ff ec 04 39 05 cd 00 0b 00 17 00 1e 40 1b 00 03 03 01 53 00 01 01 14 43 00 02 02 00 53 00 00 00 15 00 44 24 24 24 22 04 13 2b 01 10 02 23 22 02 11 10 12 33 32 12 01 10 12 33 32 12 11 10 02 23 22 02 04 39 f5 fc f4 fc f5 fb f5 fc fd 0d 7b 87 Data Ascii: J@MQE+5!H@SD$"+74632#"&LHILMHHL}INQFGSR@CD+#!JX9@SCSD$$$"+#"3232#"9{

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49839	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:08 UTC	238	OUT	GET /cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Bold-webfont.ttf HTTP/1.1 Host: webmail.unitedyacht.com Connection: keep-alive Origin: https://arthurperush.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183. 121 Safari/537.36 Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: font Referer: https://webmail.unitedyacht.com/cPanel_magic_revision_1386192030/unprotected/cpanel/fonts/open_sans/o pen_sans.min.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 05:41:08 UTC	247	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:08 GMT Server: Apache/2.4.53 (cPanel) OpenSSL/1.1.1o mod_bwlimited/1.4 Content-Type: application/octet-stream Last-Modified: Tue, 23 Mar 2021 16:37:21 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:08 GMT Content-Length: 38452 Vary: Accept-Encoding,User-Agent Connection: close
2022-05-27 05:41:08 UTC	256	IN	Data Raw: 00 01 00 00 00 13 01 00 00 04 00 30 46 46 54 4d 63 54 d3 4e 00 00 01 3c 00 00 00 1c 47 44 45 46 01 1c 00 04 00 00 01 58 00 00 00 20 47 50 4f 53 2d 72 17 42 00 00 01 78 00 00 09 9e 47 53 55 42 a0 62 88 9e 00 00 0b 18 00 00 00 a8 4f 53 2f 32 a2 49 9b dd 00 00 0b c0 00 00 00 60 63 6d 61 70 b7 6f 6c be 00 00 0c 20 00 00 02 02 63 76 74 20 2b 73 06 e0 00 00 0e 24 00 00 00 3c 66 70 67 6d 8b 0b 7a 41 00 00 0e 60 00 00 09 91 67 61 73 70 00 00 00 10 00 00 17 f4 00 00 00 08 67 6c 79 66 80 78 59 fa 00 00 17 fc 00 00 70 58 68 65 61 64 01 63 95 da 00 00 88 54 00 00 00 36 68 68 65 61 0f 15 05 89 00 00 88 8c 00 00 00 24 68 6d 74 78 31 a0 4c d4 00 00 88 b0 00 00 03 bc 6c 6f 63 61 7d 4f 9a ca 00 00 8c 6c 00 00 01 e0 6d 61 78 70 03 21 02 3c 00 00 8e 4c 00 00 00 20 6e 61 6d Data Ascii: 0FFTMcTN<GDEFX GPOS-rBxGSUBbOS/2I`cmapol cvt +s$<fpgmzA`gaspglyfxYpXheadcT6hhea$hmtx1Llo ca}Olmaxp!<L nam
2022-05-27 05:41:08 UTC	264	IN	Data Raw: 45 12 12 02 11 2b 25 06 03 23 12 37 21 01 cb 34 7c dc 41 24 01 18 d7 ca fe eb 01 0a ec 00 00 00 01 00 3d 01 a8 02 56 02 a2 00 03 00 1d 40 1a 00 00 01 01 00 4d 00 00 00 01 51 02 01 01 00 01 45 00 00 00 03 00 03 11 03 10 2b 13 35 21 15 3d 02 19 01 a8 fa fa 00 00 00 01 00 75 ff e5 01 d3 01 39 00 0b 00 12 40 0f 00 00 00 01 53 00 01 01 15 01 44 24 22 02 11 2b 37 34 36 33 32 16 15 14 06 23 22 26 75 5a 56 53 5b 5c 52 54 5c 8f 54 56 58 52 4f 5b 59 00 00 00 00 01 00 0e 00 00 03 44 05 b6 00 03 00 18 40 15 02 01 01 01 0c 43 00 00 00 0d 00 44 00 00 00 03 00 03 11 03 10 2b 09 01 21 01 03 44 fd df fe eb 02 21 05 b6 fa 4a 05 b6 00 02 00 4a ff ec 04 48 05 cd 00 0b 00 17 00 1e 40 1b 00 03 03 01 53 00 01 01 1 4 43 00 02 02 00 53 00 00 00 15 00 44 24 24 24 22 04 13 2b 01 10 Data Ascii: E+%#7!4|A$=V@MQE+5!=u9@SD$"+74632#"&uZVS[\RT\TVXRO[YD@CD+!D!JJH@SCSD$$$"+

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49841	151.101.112.193	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:09 UTC	264	OUT	GET /VCmmJUv.png HTTP/1.1 Host: i.imgur.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://arthurperush.com/css/cPanel.SharePoint_documentOnline/login.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 05:41:09 UTC	264	IN	HTTP/1.1 200 OK Connection: close Content-Length: 2759 Last-Modified: Sun, 07 Nov 2021 13:21:42 GMT ETag: "ed7d4120df814541a69c72293dca47ba" Content-Type: image/png cache-control: public, max-age=31536000 Accept-Ranges: bytes Date: Fri, 27 May 2022 05:41:09 GMT Age: 821432 X-Served-By: cache-iad-kiad7000133-IAD, cache-hhn4073-HHN X-Cache: HIT, HIT X-Cache-Hits: 1, 1 X-Timer: S1653630069.065418,VS0,VE1 Strict-Transport-Security: max-age=300 Access-Control-Allow-Methods: GET, OPTIONS Access-Control-Allow-Origin: * Server: cat factory 1.0 X-Content-Type-Options: nosniff
2022-05-27 05:41:09 UTC	265	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 61 00 00 00 55 08 02 00 00 00 d6 8f 1d 4f 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 0a 7e 49 44 41 54 78 5e ed 9c 09 6c 54 c7 19 c7 ff de 5d df f7 6d d7 76 0c 06 6c 83 31 18 87 53 40 b8 e2 36 ad 51 db 24 b4 80 5a 02 6a a2 4a b4 b4 55 d4 26 55 d4 16 21 82 5a 42 da 48 2d 55 50 13 09 a9 21 a5 55 da 08 c2 1d 4e 61 30 c5 e0 50 1b 30 b1 c1 e0 fb be bd 6b ef e1 dd 75 bf d9 9d 52 ec 7a df cc db b5 d5 95 f2 7e 7a 42 6f be b7 7e fb de 7f 8e ef fb 66 66 09 30 6f cf 83 86 67 42 de bd ab e3 a7 1a 9e d1 34 12 a3 69 24 46 d3 48 8c a6 91 18 4d 23 31 9a 46 62 34 8d c4 68 1a 89 d1 34 12 a3 69 24 c6 bf f3 35 a7 03 76 13 1c 66 5e 94 44 1f 0e 9d 01 ba 20 e8 f4 dc e2 03 94 af f9 b1 46 96 1e c4 cd c2 a2 62 a4 Data Ascii: PNGIHDRaUOgAMAa~IDATx^IT]mvl1S@6Q$ZjJU&U!ZBH-UP!UNa0P0kuRz~zBo~ff0ogB4i$FHM#1F b4h4i$5vf^D Fb
2022-05-27 05:41:09 UTC	266	IN	Data Raw: 7b 52 dc 48 2f 2c 79 e7 e6 fb d8 b3 16 61 29 cc 6f 24 e6 b2 c4 35 6e 6c d3 73 da 90 30 13 b1 e9 2c 2c 0c 8b e2 46 65 3e 7a 1b 25 ef 29 2f bd a9 d2 a8 09 fb aa c4 d9 06 75 c9 23 bf c3 cd 13 30 b5 c0 40 fe c2 95 31 4c 88 3b c6 a1 de 31 62 c4 9b 57 11 9b ec b2 7a e6 f2 c7 f8 e8 75 76 c3 b9 45 58 be 11 c9 d3 58 3e 38 86 51 84 46 a9 70 b8 43 03 d8 5d 04 2b 55 95 d2 2a ae 74 4e 4b 75 9e b9 0c 91 71 bc a8 40 e9 51 94 1e 86 65 00 41 b1 6c 7c a5 af 67 89 d5 44 87 1b f2 68 c9 79 88 8a e7 45 05 2a cf 32 81 a6 2d c4 fa 9f 60 de 2a 16 1f 87 47 8f 3d 62 d4 45 24 37 cf c0 d8 a9 2c 90 1b b9 9b 3a ec 48 ca 11 3f 01 0d 19 a7 df 82 c3 21 eb 7d 08 bb 19 f9 eb a0 17 b9 73 aa f3 c6 5b 18 e9 c5 97 b7 4b e5 bd 42 fa 3b 71 e1 80 e4 02 b7 64 3b b2 21 49 62 08 a4 44 a1 fb 21 f3 53 Data Ascii: {RH/,ya)o$5nls0,,Fe>z%)/u#0@1L;1bWzuvEXX>8QFpC]+U*tNKuq@QeAl|gDhyE*2-`*G=bE$7,:H?!}s[KB; qd;!IbD!S
2022-05-27 05:41:09 UTC	268	IN	Data Raw: 14 38 de 44 99 00 00 00 00 49 45 4e 44 ae 42 60 82 Data Ascii: 8DIENDB`

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49846	151.101.112.193	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:09 UTC	268	OUT	GET /VCmmJUv.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: i.imgur.com

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:09 UTC	268	IN	HTTP/1.1 200 OK Connection: close Content-Length: 2759 Last-Modified: Sun, 07 Nov 2021 13:21:42 GMT ETag: "ed7d4120df814541a69c72293dca47ba" Content-Type: image/png cache-control: public, max-age=31536000 Accept-Ranges: bytes Date: Fri, 27 May 2022 05:41:09 GMT Age: 821433 X-Served-By: cache-iad-kiad7000133-IAD, cache-hhn4049-HHN X-Cache: HIT, HIT X-Cache-Hits: 1, 1 X-Timer: S1653630070.823414,VS0,VE1 Strict-Transport-Security: max-age=300 Access-Control-Allow-Methods: GET, OPTIONS Access-Control-Allow-Origin: * Server: cat factory 1.0 X-Content-Type-Options: nosniff
2022-05-27 05:41:09 UTC	269	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 61 00 00 00 55 08 02 00 00 00 d6 8f 1d 4f 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 0a 7e 49 44 41 54 78 5e ed 9c 09 6c 54 c7 19 c7 ff de 5d df f7 6d d7 76 0c 06 6c 83 31 18 87 53 40 b8 e2 36 ad 51 db 24 b4 80 5a 02 6a a2 4a b4 b4 55 d4 26 55 d4 16 21 82 5a 42 da 48 2d 55 50 13 09 a9 21 a5 55 da 08 c2 1d 4e 61 30 c5 e0 50 1b 30 b1 c1 e0 fb be bd 6b ef e1 dd 75 bf d9 9d 52 ec 7a df cc db b5 d5 95 f2 7e 7a 42 6f be b7 7e fb de 7f 8e ef fb 66 66 09 30 6f cf 83 86 67 42 de bd ab e3 a7 1a 9e d1 34 12 a3 69 24 46 d3 48 8c a6 91 18 4d 23 31 9a 46 62 34 8d c4 68 1a 89 d1 34 12 a3 69 24 c6 bf f3 35 a7 03 76 13 1c 66 5e 94 44 1f 0e 9d 01 ba 20 e8 f4 dc e2 03 94 af f9 b1 46 96 1e c4 cd c2 a2 62 a4 Data Ascii: PNGIHDRaUOgAMAa~IDATx^IT]mvl1S@6Q$ZjJU&U!ZBH-UP!UNa0P0kuRz~zBo~ff0ogB4i$FHM#1F b4h4i$5vf^D Fb
2022-05-27 05:41:09 UTC	270	IN	Data Raw: 7b 52 dc 48 2f 2c 79 e7 e6 fb d8 b3 16 61 29 cc 6f 24 e6 b2 c4 35 6e 6c d3 73 da 90 30 13 b1 e9 2c 2c 0c 8b e2 46 65 3e 7a 1b 25 ef 29 2f bd a9 d2 a8 09 fb aa c4 d9 06 75 c9 23 bf c3 cd 13 30 b5 c0 40 fe c2 95 31 4c 88 3b c6 a1 de 31 62 c4 9b 57 11 9b ec b2 7a e6 f2 c7 f8 e8 75 76 c3 b9 45 58 be 11 c9 d3 58 3e 38 86 51 84 46 a9 70 b8 43 03 d8 5d 04 2b 55 95 d2 2a ae 74 4e 4b 75 9e b9 0c 91 71 bc a8 40 e9 51 94 1e 86 65 00 41 b1 6c 7c a5 af 67 89 d5 44 87 1b f2 68 c9 79 88 8a e7 45 05 2a cf 32 81 a6 2d c4 fa 9f 60 de 2a 16 1f 87 47 8f 3d 62 d4 45 24 37 cf c0 d8 a9 2c 90 1b b9 9b 3a ec 48 ca 11 3f 01 0d 19 a7 df 82 c3 21 eb 7d 08 bb 19 f9 eb a0 17 b9 73 aa f3 c6 5b 18 e9 c5 97 b7 4b e5 bd 42 fa 3b 71 e1 80 e4 02 b7 64 3b b2 21 49 62 08 a4 44 a1 fb 21 f3 53 Data Ascii: {RH/,ya)o$5nls0,,Fe>z%)/u#0@1L;1bWzuvEXX>8QFpC]+U*tNKuq@QeAl|gDhyE*2-`*G=bE$7,:H?!}s[KB; qd;!IbD!S
2022-05-27 05:41:09 UTC	271	IN	Data Raw: 14 38 de 44 99 00 00 00 00 49 45 4e 44 ae 42 60 82 Data Ascii: 8DIENDB`

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49849	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:10 UTC	271	OUT	GET /cPanel_magic_revision_1547665285/unprotected/cpanel/images/icon-username.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: webmail.unitedyacht.com
2022-05-27 05:41:10 UTC	272	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:10 GMT Server: Apache/2.4.53 (cPanel) OpenSSL/1.1.1o mod_bwlimited/1.4 Content-Type: image/png Last-Modified: Wed, 16 Jan 2019 19:01:25 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:10 GMT Content-Length: 320 Connection: close
2022-05-27 05:41:10 UTC	272	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 14 00 00 00 14 08 06 00 00 00 8d 89 1d 0d 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 88 00 00 00 09 70 48 59 73 00 00 0b 12 00 00 0b 12 01 d2 dd 7e fc 00 00 00 1c 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 46 69 72 65 77 6f 72 6b 73 20 43 53 34 06 b2 d3 a0 00 00 00 15 74 45 58 74 43 72 65 61 74 69 6f 6e 20 54 69 6d 65 00 36 2f 32 39 2f 31 31 13 6b 0a 4d 00 00 00 99 49 44 41 54 38 cb 63 f8 ff ff 3f 03 35 31 82 81 06 d8 6c 3c d9 81 d8 0a 88 e3 80 b8 18 4a cb 82 c4 41 f2 e4 18 18 0e 35 08 1d 87 93 6b 60 31 2e 3c 0c 0d 04 6a 32 c6 67 20 48 9e 54 03 ad 08 18 68 45 aa 81 2a 78 0c cb 01 c9 93 13 86 b8 5c a9 4d 6e a4 b0 23 25 6a 18 8e 83 c9 93 6c 20 0e 57 5a 51 6a a0 3f 9a 81 fe 24 1b 08 8d Data Ascii: PNGIHDRsBIT|dpHYs~tEXtSoftwareAdobe Fireworks CS4tEXtCreation Time6/29/11kMIDAT8c?51l<JA5k`1. <j2g HThE*x\Mn#%jl WZQj?$

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49848	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:10 UTC	271	OUT	GET /cPanel_magic_revision_1458739301/unprotected/cpanel/images/webmail-logo.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: webmail.unitedyacht.com
2022-05-27 05:41:10 UTC	272	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:10 GMT Server: Apache/2.4.53 (cPanel) OpenSSL/1.1.1o mod_bwlimited/1.4 Content-Type: image/svg+xml Last-Modified: Wed, 16 Jan 2019 19:01:25 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:10 GMT Content-Length: 5360 Vary: Accept-Encoding,User-Agent Connection: close
2022-05-27 05:41:10 UTC	273	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 34 36 32 70 74 22 20 68 65 69 67 68 74 3d 22 33 32 30 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 34 36 32 20 32 34 30 22 3e 3c 64 65 66 73 3e 3c 63 6c 69 70 50 61 74 68 20 69 64 3d 22 61 22 3e 3c 70 61 74 68 20 64 3d 22 4d 31 33 33 39 20 30 68 31 32 32 2e 34 34 76 32 34 30 48 31 33 33 39 7a 6d 30 20 30 20 22 2f 3e 3c 2f 63 6c 69 70 50 61 74 68 3e 3c 2f 64 65 66 73 3e 3c 70 61 74 68 20 64 3d 22 4d 33 36 35 2e 31 30 32 20 31 34 2e 33 39 38 6c 2d 34 33 2e 32 30 34 20 31 36 30 2e 32 30 34 63 2d 32 2e 35 39 37 20 39 2e 35 39 37 2d 36 2e 35 39 37 20 31 38 2e 34 35 2d 31 32 20 32 36 2e 35 34 36 2d 35 2e 33 39 38 20 38 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="1462pt" height="320" viewBox="0 0 1462 240"><defs><clipPath id="a"><path d="M1339 0h122.44v240H1339zm0 0"/></clipPath></defs><path d="M365.102 14.398l-43.204 160.204c-2.597 9.597-6.597 18.45-12 26.546-5.398 8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49851	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:10 UTC	278	OUT	GET / oPSIzNTIwdCIgaGVpZ2h0PSIzMjAiIHZpZXdCb3g9IjAgMCAzNTkgMjQwIj48ZGVmcz48Y2xpcFBhdGggaWQ9ImEiP jxwYXRoIGQ9Ik0xMjMgMGgyMzUuMzd2MjQwSDEyM3ptMCAwIi8+PC9jbGlwUGF0aD48L2RlZnM+PHBhdGggZD0iTTg 5LjY5IDU5LjEwMmg2Ny44MDJsLTEwLjUgNDAuMmMtMS42MDUgNS42LTQuNjA1IDEwLjEtOSAxMy41LTQ uNDAyIDMuNC05LjUwNCA1LjA5Ni0xNS4zIDUuMDk2aC0zMS41Yy03LjIgMC0xMy41LjEwMi0zOC4xMTg S41MDUgNC4yLTkuMzUzIDkuOTA0LTExLjU1MiAxNy4xMDMtMS40IDUuNDAzLTEuNTUgMTAuNS0uNDUgM TUuMzAyIDEuMDk4IDQuNzk2IDMuMDQ3IDkuNDUgNS44NTIgMTIuNzUgMi43OTcgMy43MDMgNi40IDIyNjUyIDEwLjc 5NyA4Ljg1IDQuMzk3IDIuMiA5LjE5OCAzLjI5OCAxNC40IDMuMjk4aDE5LjJjMy42MDMgMCA2LjU0NyAxLjQ1MyA4L jg1MiA0LjM1MiAyLjI5NyAyLjkwMiAyLjk0NSA2LjE0OCAxLjk1IDkuNzVsLTEyIDQ0LjM5OGgtMjFjLTE0LjQwMyA wLTI3LjY1My0zLjE0OC0zOS43NS05LjQ1LTEyLjEwMi02LjMtMjIuMTUzLTE0LjY0OC0zMC4xNTMtMjUuMDUtOC0xM C4zOTUtMTMuNDU0LTIyLjI0Ni0xNi4zNS0zNS41NDctMi45LTEzLjMtMi41NS0yNi45NSAxLjA1Mi00MC45NTNsMS4 yLTQuNWMyLjU5Ny05LjYwMiA2LjY0OC0xOC40NSAxMi4xNDgtMjYuNTUgNS41LTguMDk4IDEyLTE1IDE5LjUtMjAuN yA3LjUtNS43IDE1Ljg1LTEwLjE0OCAyNS4wNS0xMy4zNzNIgOS4yLTMuMTk1IDE4Ljc5Ny00LjQzNS0xLjA1Mi00Ljc 2liBmaWxsPSIjZmY2YzJli8+PGcgY2xpcC1wYXRoPSJ1cmwoI2Eplj48cGF0aCBkPSJNMTIzLjg5IDI0MEwxODIuO TkgMTguNjAyYzEuNTk4LTUuNTk4IDQuNTk4LTEwLjA5OCA1LTEzLjVDMTk2LjM4OCAxLjcgMy4yOTQuNjAyLjQ4NCAwIDIwNy4 yODggMGg2Mi43YzE0LjQwMyAwIDI3LjY1IDMuMTQ4IDM5Ljc1IDIuMTAyIDYuMyAyMi4xNTMgMTQuNjQuNjU1I DMwLjE1MyAyNS4wNSA3Ljk5NyAxMC40MDIgMTMuNSAyMi4yNTQgMTYuNSAzNS41NSAzIDEzLjMwNSAyL jU5NCAyNi45NTQtMS4yMDIgNDAuOTVsLTEuMiA0LjVjLTIuNTk3IDkuNjAyLTYuNTk3IDE4LjQ1LTEyIDI2LjU1LTU uMzk4IDguMDk4LTEzLjg0NyAxNS4wNTItMTkuMTUzMzQ3IDIwLjg0OC03LjUgNS44MDUtMTUuODU1IDEwLjMwNS0yNS4wNS SAxMy41LTkuMiAzLjIwNC0xOC44MDUgNC44MDUtMjguguODA1aC01NC4yOTdsMTAuOC00MC41Y zEuNi01LjQwMiA0LjYtOS44IDktMTMuMjAzIDQuMzk2LTMuMzk4IDNk3LTUuMTAyIDE1LjMwMi01LjEwMmgxNy4 zOThjNy4yIDAgMTMuNjUzLTIuMiAxOS4zNTItNi41OTcgNS42OTUtNC4zOTggOS40NDUtMTAuMDk3IDExLjI1LTE3L jEgMS4zOTQtNC45OTcgMS41NDctOS45LjQ0NS0xNC43LTEuMS00LjgtMy4wNS05LjA0Ny01LjgtMy4yOTUtNi40MDItNi42OTUtNi42MDItNi42OTUtMTAuNzk2LTktNC40MDYtMi4yOTctOS4yMDYtMy40NS0xNC40MDItMy40MDctMi40MDYtNC40MDItMy40NS0xNC40MDItMy40NUgyMzMuM zlsLTQzLjggMTYyLjkwM2MtMS42MDYgNS40LTQuNjA2IDkuNzk3LTkgMTMuMTk1LTQuNDAzIDMuNDA3LTkuNDA2IDIDU uMTAyLTE1IDUuMTAyaC00MS43liBmaWxsPSIjZmY2YzJli8+PC9nPjwvc3ZnPgo= HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: webmail.unitedyacht.com

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:11 UTC	281	IN	HTTP/1.1 308 Moved Date: Fri, 27 May 2022 05:41:11 GMT Server: Apache/2.4.53 (cPanel) OpenSSL/1.1.1o mod_bwlimited/1.4 Content-length: 2373 Location: /data%3aimage/svg%2bxml%3bbase64%2cPHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwM C9zdmciIHdpZHRoPSIzNTlwdCIgaGVpZ2h0PSIzMjAiIHZpZXdCb3g9IjAgMCAzNTkgMjQwIj48ZGVmcz48Y2xpcFB hdGggaWQ9ImEiPjxwYXRoIGQ9Ik0xMjMgMGgyMzUuMzd2MjQwSDEyM3ptMCAwIi8%2bPC9jbGlwUGF0aD48L2RlZnM %2bPHBhdGggZD0iTTg5LjY5IDU5LjEwMmg2Ny44MDJsLTEwLjUgNDAuMmMtMS42MDUgNS42LTQuNjA1I DEwLjEtOSAxMy41LTQuNDAyIDMuNC05LjUwNCA1LjA5Ni0xNS4zIDUuMDk2aC0zMS41Yy03LjIgMC0xMy41NSAyLjE wMi0xOS4wNSA2LjMtNS41MDUgNC4yLTkuMzUzIDkuOTA0LTExLjU1MiAxNy4xMDMtMS40IDUuNDAzLTE uNTUgMTAuNS0uNDUgMTUuMzAyIDEuMDk4IDQuNzk2IDMuMDQ3IDkuNDQtNC44NzUgMTIuNTUgMTIuNTE0L jY0OC0zMC4xNTMtMjUuMDUtOC0xMC4zOTUtMTMuNDU0LTIyLjI0Ni0xNi4zNS0zNS41NDctMi45LTEzLjMtMi41NS0 yNi45NSAxLjA1Mi00MC45NTNsMS4yLTQuNWMyLjU5Ny05LjYwMiA2LjY0OC0xOC40NSAxMi4xNDgtMjYuNTUgNS41L TguMDk4IDEyLTE1IDE5LjUtMjAuNyA3LjUtNS43IDE1Lg1LTEwLjE0OCAyNS4wNS0xMy4zNTIgOS4yLTMuMTk1IDE 4Ljc5Ny00Ljc5NiAyOC44LTQuNzk2IiBmaWxsPSIjZmY2YzJjIi8%2bPGcgY2xpcC1wYXRoPSJ1cmwoI2EpIj48cGF 0aCBkPSJNMTIzLjg5IDI0MEwxODIuOTkgMTguNjAyYzEuNTk4LTUuNTk4IDQuNTk4LTEwLjA5OCA5LTEzLjVDMTk2L jM4OCAxLjcgMjAxLjQ4NCAwIDIwNy4yODggMTg2Mi43YzE0LjQwMyAwIDI3LjY1IDMuMTQ4IDM5Ljc1IDkuNDUgMTI uMTAyIDYuMyAyMi4xNTMgMTQuNjU1IDMwLjE1MyAyNS4wNSA3Ljk5NyAxMC40MDIgMTMuNSAyMi4yLTYuNTk3IDkuNjAyL TYuNTk3IDE4LjQ1LTEyIDI2LjU1LTUuMzk4IDguMDk4LTEzLjg0LTAuNzk2IDI0LjUgNS4xNTItMTMuNTk3IDkuNjAyL 4MDUtMTUuODU1IDEwLjMwNS0yNS4wNSAxMy41LTkuMiAzLjIwNC0xOC44MDUgMTMuMjguODA1aC01NC4yOTdsMTAuOD3L TUuMTAyIDE1LjMwMi01LjEwMmgxNy4zOThjNy4yIDAgMTMuNjUzLTIuMiAxOS4zNTItNi41OTcgNS42OTUtNC4zOTg gOS40NDUtMTAuMDk3IDExLjI1LTE3LjEgMS4zOTQtNC45OTcgMS41NDctOS5LjQ0NS0xNC43LTEuMS00LjgtNS 7a4e54 6c77 6443 4967 6147 5670 5a32 6830 5053 497a 4d6a 4177 4d43 397a 6463 6949 4864 705a 4852 6f50 5349 7a4e 546c 7764 4349 6761 4756 705a 3268 3050 5349 7a4d 6a41 6949 4854 705a 5864 4362 3367 3949 6a 41674d434 17a4e546b 674d6a51 7749 6a34 385a 4756 6d63 7a34 3859 3278 7063 4642 6864 4767 6761 5751 3949 6d45 6950 6a78 7759 5852 6f49 4751 3949 6b30 784d 6a Data Ascii: <html><head><META HTTP-EQUIV="refresh" CONTENT="2;URL=/data%3aimage/svg%2bxml%3bbase64%2 cPHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHdpZHRoPSIzNTlwdCIgaGVpZ2h0PSIzMjAiI HZpZXdCb3g9IjAgMCAzNTkgMjQwIj48ZGVmcz48Y2xpcFBhdGggaWQ9ImEiPjxwYXRoIGQ9Ik0xMj
2022-05-27 05:41:11 UTC	283	IN	Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 72 65 66 72 65 73 68 22 20 43 4f 4e 54 45 4e 54 3d 22 32 3b 55 52 4c 3d 2f 64 61 74 61 25 33 61 69 6d 61 67 65 2f 73 76 67 25 32 62 78 6d 6c 25 33 62 62 61 73 65 36 34 25 32 63 50 48 4e 32 5a 79 42 34 62 57 78 75 63 7a 30 69 61 48 52 30 63 44 6f 76 4c 33 64 33 64 79 35 33 4d 79 35 76 63 6d 63 76 4d 6a 41 77 4d 43 39 7a 64 6d 63 69 49 48 64 70 5a 48 52 6f 50 53 49 7a 4e 54 6c 77 64 43 49 67 61 47 56 70 5a 32 68 30 50 53 49 7a 4d 6a 41 69 49 48 5a 70 5a 58 64 43 62 33 67 39 49 6a 41 67 4d 43 41 7a 4e 54 6b 67 4d 6a 51 77 49 6a 34 38 5a 47 56 6d 63 7a 34 38 59 32 78 70 63 46 42 68 64 47 67 67 61 57 51 39 49 6d 45 69 50 6a 78 77 59 58 52 6f 49 47 51 39 49 6b 30 78 4d 6a Data Ascii: <html><head><META HTTP-EQUIV="refresh" CONTENT="2;URL=/data%3aimage/svg%2bxml%3bbase64%2 cPHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHdpZHRoPSIzNTlwdCIgaGVpZ2h0PSIzMjAiI HZpZXdCb3g9IjAgMCAzNTkgMjQwIj48ZGVmcz48Y2xpcFBhdGggaWQ9ImEiPjxwYXRoIGQ9Ik0xMj

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49819	138.59.135.12	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:05 UTC	4	OUT	GET /css/cPanel.SharePoint_documentOnline/login.html HTTP/1.1 Host: arthurperush.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183. 121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig ned-exchange;v=b3;q=0.9 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Referer: http://v2.bpkbsaya.com/wp-includes/css/cPanel.SharePoint_documentOnline/redirecting.php Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 05:41:05 UTC	5	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:05 GMT Server: Apache Last-Modified: Fri, 27 May 2022 00:31:43 GMT Accept-Ranges: bytes Content-Length: 37837 Connection: close Content-Type: text/html

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:05 UTC	5	IN	Data Raw: ef bb bf 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 64 69 72 3d 22 6c 74 72 22 3e 0d 0a 0d 0a 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f 67 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 74 72 61 6e 73 6c 61 74 65 Data Ascii: <!DOCTYPE html><html lang="en" dir="ltr"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <meta name="google" content="notranslate
2022-05-27 05:41:05 UTC	13	IN	Data Raw: 6e 6c 22 3e 4e 65 64 65 72 6c 61 6e 64 73 3c 2f 61 3e 3c 2f 64 69 76 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 2f 3f 6c 6f 63 61 6c 65 3d 6e 6f 22 3e 4e 6f 72 77 65 67 69 61 6e 3c 2f 61 3e 3c 2f 64 69 76 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 6 6 3d 22 2f 3f 6c 6f 63 61 6c 65 3d 70 6c 22 3e 70 6f 6c 73 6b 69 Data Ascii: nl">Nederlands</div> <div class="locale-cell">Norwegian</div> <div class="locale-cell"><a href="/?locale=pl">polski

2022-05-27 05:41:05 UTC	21	IN	Data Raw: 64 20 62 61 63 6b 20 74 68 65 20 49 44 20 74 6f 6b 65 6e 2e 20 0d 0a 0d 0a 5c 78 33 63 61 20 68 72 65 66 3d
			5c 22 5c 22 3e 4c 6f 67 20 69 6e 20 74 6f 20 20 61 67 61 69 6e 2e 5c 78 33 63 2f 61 3e 20 49 66 20 74 68 69 73 20 63 6f
			6e 64 69 74 69 6f 6e 20 70 65 72 73 69 73 74 73 2c 20 63 6f 6e 74 61 63 74 20 79 6f 75 72 20 73 79 73 74 65 6d 20 61
			64 6d 69 6e 69 73 74 72 61 74 6f 72 2e 22 7d 3b 0d 0a 0d 0a 20 20 20 20 77 69 6e 64 6f 77 2e 49 53 5f 4c 4f 47 4f 55 54
			20 3d 20 66 61 6c 73 65 3b 0d 0a 0d 0a 0d 0a 2f 2f 6c 6f 67 69 6e 2e 6a 73 0d 0a 22 75 73 65 20 73 74 72 69 63 74 22
			3b 76 61 72 20 46 41 44 45 5f 44 55 52 41 54 49 4f 4e 3d 2e 34 35 3b 76 61 72 20 46 41 44 45 5f 44 45 4c 41 59 3d 32 3
			0 3b 76 61 72 20 41 4a 41 58 5f 54 49 4d 45 4f 55 54 3d 33 65 34
			Data Ascii: d back the ID token. \x3ca href=\"\">Log in to again.\x3c/a> If this condition persists, contact your system
			administrator."}; window.IS_LOGOUT = false;//login.js"use strict";var FADE_DURATION=.45;var FADE_DELAY=20;var
			AJAX_TIMEOUT=3e4

2022-05-27 05:41:05 UTC	28	IN	Data Raw: 65 6e 74 2e 62 6f 64 79 2e 6f 6e 6b 65 79 75 70 3d 66 75 6e 63 74 69 6f 6e 28 29 0d 0a 0d 0a 7b 4c 4f 47 49 4e 5f 53 55 42 4d 49 54 5f 4f 4b 3d 74 72 75 65 7d 3b 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 2e 6f 6e 6d 6f 75 73 65 64 6f 77 6e 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 4c 4f 47 49 4e 5f 53 55 42 4d 49 54 5f 4f 4b 3d 74 72 75 65 7d 3b 66 75 6e 63 74 69 6f 6e 20 64 6f 5f 6c 6f 67 69 6e 28 29 7b 69 66 28 4c 4f 47 49 4e 5f 53 55 42 4d 49 54 5f 4f 4b 29 7b 4c 4f 47 49 4e 5f 53 55 42 4d 49 54 5f 4f 4b 3d 66 61 6c 73 65 3b 69 66 0d 0a 0d 0a 28 6c 6f 67 69 6e 5f 75 73 65 72 6e 61 6d 65 5f 65 6c 2e 76 61 6c 75 65 2e 6c 65 6e 67 74 68 3d 3d 3d 30 29 7b 73 68 6f 77 5f 73 74 61 74 75 73 28 4d 45 53 53 41 47 45 53 2e 6e 6f 5f 75 73 65 72 6e 61 6d 65 2c 22 65 72 72 Data Ascii: ent.body.onkeyup=function(){LOGIN_SUBMIT_OK=true};document.body.onmousedown=function(){L OGIN_SUBMIT_OK=true};function do_login(){if(LOGIN_SUBMIT_OK){LOGIN_SUBMIT_OK=false;if(login_username _el.value.length===0){show_status(MESSAGES.no_username,"err
2022-05-27 05:41:06 UTC	36	IN	Data Raw: 31 22 3a 22 41 73 69 61 2f 42 61 6b 75 22 2c 22 32 37 30 2c 30 22 3a 22 41 73 69 61 2f 4b 61 62 75 6c 22 2c 22 33 30 30 2c 31 22 3a 22 41 73 69 61 0d 0a 0d 0a 2f 59 65 6b 61 74 65 72 69 6e 62 75 72 67 22 2c 22 33 30 30 2c 30 22 3a 22 41 73 69 61 2f 4b 61 72 61 63 68 69 22 2c 22 33 33 30 2c 30 22 3a 22 41 73 69 61 2f 4b 6f 6c 6b 61 74 61 22 2c 22 33 34 35 2c 30 22 3a 22 41 73 69 61 2f 4b 61 74 68 6d 61 6e 64 75 22 2c 22 33 36 30 2c 30 22 3a 22 41 73 69 61 2f 44 68 61 6b 61 22 2c 22 33 36 30 2c 31 22 3a 22 41 73 69 61 2f 4f 6d 73 6b 22 2c 22 33 39 30 2c 30 22 3a 22 41 73 69 6 1 2f 52 61 6e 67 6f 6f 6e 22 2c 22 34 32 30 2c 31 22 3a 22 41 73 69 61 2f 4b 72 0d 0a 0d 0a 61 73 6e 6f 79 61 72 73 6b 2 2 2c 22 34 32 30 2c 30 22 3a 22 41 73 69 61 2f 4a 61 6b 61 72 74 Data Ascii: 1":"Asia/Baku","270,0":"Asia/Kabul","300,1":"Asia/Yekaterinburg","300,0":"Asia/Karachi","330,0":"Asia/Kolkat a","345,0":"Asia/Kathmandu","360,0":"Asia/Dhaka","360,1":"Asia/Omsk","390,0":"Asia/Rangoon","420,1":"Asia/Kras noyarsk","420,0":"Asia/Jakart

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49850	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:10 UTC	280	OUT	GET /cPanel_magic_revision_1547665285/unprotected/cpanel/images/icon-password.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240. 183 Safari/537.36 Host: webmail.unitedyacht.com
2022-05-27 05:41:11 UTC	285	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:11 GMT Server: Apache/2.4.53 (cPanel) OpenSSL/1.1.1o mod_bwlimited/1.4 Content-Type: image/png Last-Modified: Wed, 16 Jan 2019 19:01:25 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:11 GMT Content-Length: 450 Connection: close
2022-05-27 05:41:11 UTC	286	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 14 00 00 00 14 08 06 00 00 00 8d 89 1d 0d 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 88 00 00 00 09 70 48 59 73 00 00 0b 12 00 00 0b 12 01 d2 dd 7e fc 00 00 00 1c 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 46 69 72 65 77 6f 72 6b 73 20 43 53 34 06 b2 d3 a0 00 00 00 1 5 74 45 58 74 43 72 65 61 74 69 6f 6e 20 54 69 6d 65 00 36 2f 32 39 2f 31 31 13 6b 0a 4d 00 00 01 1b 49 44 41 54 38 cb 63 f8 ff ff 3f 03 35 31 2a 07 09 b0 d9 78 b2 03 b1 15 10 e7 00 71 31 14 a7 82 c4 40 f2 24 19 08 32 8c dd d6 2b 0e 64 88 8 0 4b 60 92 7e 4c ba 2b 08 0b bb 07 c7 40 0d f6 27 c9 40 0e 5b 2f 47 90 46 97 dc 32 2b a0 b8 30 10 f3 40 b1 20 48 0c 6a a8 15 29 2e 2c 96 f6 89 08 07 8a 71 32 a0 01 90 98 42 60 4c 20 a7 Data Ascii: PNGIHDRsBIT|dpHYs~tEXtSoftwareAdobe Fireworks CS4tEXtCreation Time6/29/11kMIDAT8c?51*xq1 @$2+dK`~L+@'@[/GF2+0@ Hj).,q2B`L

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49852	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:11 UTC	286	OUT	GET /data%3aimage/svg%2bxml%3bbase64%2cPHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmc iIHdpZHRoPSIzNTlwdCIgaGVpZ2h0PSIzMjAiIHZpZXdCb3g9IjAgMCAzNTkgMjQwIj48ZGVmcz48Y2xpcFBhdGgga WQ9ImEiPjxwYXRoIGQ9Ik0xMjMgMGgyMzUuMzd2MjQwSDEyM3ptMCAwIi8%2bPC9jbGlwUGF0aD48L2R lZnM%2bPHBhdGggZD0iTTg5LjY5IDU5LjEwMmg2Ny44MDJsLTEwLjUgNDAuMmMtMS42MDUgNS42LTQuN jA1IDEwLjEtOSAxMy41LTQuNDAyIDMuNC05LjUwNCA1LjA5Ni0xNS4zIDUuMDk2aC0zMS41Yy03LjIgMC0xMy41NSA yLjEwMi0xOS4wNSA2LjMtNS41MDUgNC4yLTkuMzUzIDkuOTA0LTExLjU1MiAxNy4xMDMtMS40IDUuNDAzLTEuNTUgM TAuNS0uNDUgMTUuMzAyIDEuMDk4IDQuNzk2IDMuMDQ3IDkuMDUgNS44NTIgMTIuNzUgMi43OTcgMy43M DMgNi40IDYuNjUyIDEwLjc5NyA4Ljg1IDQuMzk3IDIuMiA5LjE5OCAzLjI5OCAxNC40IDMuMjk4aDE5LjJjMy42MDI gMCA2LjU0NyAxLjQ1MyA4Ljg1MiA0LjM1MiAyLjI5NyAyLjkwMiAyLjk0NSA2LjE0OCAxLjk1IDkuNzVsLTEyIDQ0L jM5OGgtMjFjLTE0LjQwMyAwLTI3LjY1My0zLjE0OC0zOS43NS05LjQ1LTEyLjEwMi02LjMtMjIuMTUzLTE0LjY0OC0 zMC4xNTMtMjUuMDUtOC0xMC4zOTUtMTMuNDU0LTIyLjI0Ni0xNi4zNS0zNS41NDctMi45LTEzLjMtMi41NS0yNi45N SAxLjA1Mi00MC45NTNsMS4yLTQuNWMyLjU5Ny05LjYwMiA2LjY0OC0xOC40NSAxMi4xNDgtMjYuNTUgNS41LTguMDk 4IDEyLTE1IDE5LjUtMjAuNyA3LjUtNS43IDE1Ljg1LTEwLjE0OCAyNS4wNS0xMy4zNTIgOS4yLTMuMTk1IDE4Ljc5N y00Ljc5NiAyOC44LTQuNzk2IiBmaWxsPSIjZmY2YzJjIi8%2bPGcgY2xpcC1wYXRoPSJ1cmwoI2EpIj48cGF0aCBkP SJNMTIzLjg5IDI0MEwxODIuOTkgMTguNjAyYzEuNTk4LTUuNTk4IDQuNTk4LTEwLjA5OCA5LTEzLjVDMTk2LjM4OCA xLjcgMjAxLjQ4NCAwIDIwNy4yODggMGg2Mi43YzE0LjQwMyAwIDI3LjY1IDMuMTQ4IDM5Ljc1IDkuNDUgMTIuMTAyI DYuMyAyMi4xNTMgMTQuNjU1IDMwLjE1MyAyNS4wNSA3Ljk5NyAxMC40MDIgMTMuNSAyMi4yNTQgMTYuN SAzNS41NSAzIDEzLjMwNSAyLjU5NCAyNi45NTQtMS4yMDIgNDAuOTVsLTEuMiA0LjVjLTIuNTk3IDkuNjAyLTYuNTk 3IDE4LjQ1LTEyIDI2LjU1LTUuMzk4IDguMDk4LTExLjg0NyAxNS4wNTItMTkuMzQ3IDIwLjg0OC03LjUgNS44MDUtM TUuODU1IDEwLjMwNS0yNS4wNSAxMy41LTkuMiAzLjIwNC0xOC44MDUgNC44MDUtMjguODA1IDQuODA1a C01NC4yOTdsMTAuOC00MC41YzEuNi01LjQwMiA0LjYtOS44IDktMTMuMjAzIDQuMzk2LTMuMzk4IDkuNDk3LTUuMTA yIDE1LjMwMi01LjEwMmgxNy4zOThjNy4yIDAgMTMuNjUzLTIuMiAxOS4zNTItNi41OTcgNS42OTUtNC4zOTggOS40N DUtMTAuMDk3IDExLjI1LTE3LjEgMS4zOTQtNC45OTcgMS41NDctOS45LjQ0NS0xNC43LTEuMS00LjgtMy4wNS05LjA 0Ny01Ljg0OC0xMi43NS0yLjgtMy42OTUtNi40MDItNi42OTUtMTAuNzk2LTktNC40MDYtMi4yOTctOS4yMDYtMy40N S0xNC40MDItMy40NUgyMzMuMzlsLTQzLjggMTYyLjkwM2MtMS42MDYgNS40LTQuNjA2IDkuNzk3LTkgMTMuMTk1LTQ uNDAzIDMuNDA3LTkuNDA2IDUuMTAyLTE1IDUuMTAyaC00MS43IiBmaWxsPSIjZmY2YzJjIi8%2bPC9nPjwvc3ZnPgo %3d HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240. 183 Safari/537.36 Host: webmail.unitedyacht.com Connection: Keep-Alive
2022-05-27 05:41:11 UTC	289	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:11 GMT Server: Apache/2.4.53 (cPanel) OpenSSL/1.1.1o mod_bwlimited/1.4 Content-Type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 40228 Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: webmailsession=%3aQReor97DnwAqjal_%2c13b0bb0cd62842e6465939c595d9038e; HttpOnly; path=/; port=443; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=webmail.unitedyacht.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.unitedyacht.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.unitedyacht.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=443; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: imp_key=expired; HttpOnly; domain=webmail.unitedyacht.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.unitedyacht.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.unitedyacht.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 27-May-2023 05:41:11 GMT; path=/; port=443; secure Vary: Accept-Encoding,User-Agent Connection: close
2022-05-27 05:41:11 UTC	290	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 64 69 72 3d 22 6c 74 72 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f Data Ascii: <!DOCTYPE html><html lang="en" dir="ltr"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1"> <meta name="goo

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:11 UTC	297	IN	Data Raw: 79 4d 69 34 79 4e 54 51 67 4d 54 59 75 4e 53 41 7a 4e 53 34 31 4e 53 41 7a 49 44 45 7a 4c 6a 4d 77 4e 53 41 79 4c 6a 55 35 4e 43 41 79 4e 69 34 35 4e 54 51 74 4d 53 34 79 4d 44 49 67 4e 44 41 75 4f 54 56 73 4c 54 45 75 4d 69 41 30 4c 6a 56 6a 4c 54 49 75 4e 54 6b 33 49 44 6b 75 4e 6a 41 79 4c 54 59 75 4e 54 6b 33 49 44 45 34 4c 6a 51 31 4c 54 45 79 49 44 49 32 4c 6a 55 31 4c 54 55 75 4d 7a 6b 34 49 44 67 75 4d 44 6b 34 4c 54 45 78 4c 6a 67 30 4e 79 41 78 4e 53 34 77 4e 54 49 74 4d 54 6b 75 4d 7a 51 33 49 44 49 77 4c 6a 67 30 4f 43 30 33 4c 6a 55 67 4e 53 34 4d 44 55 74 4d 54 55 75 4f 44 55 31 49 44 45 77 4c 6a 4d 77 4e 53 30 79 4e 53 34 77 4e 53 41 78 4d 79 34 31 4c 54 6b 75 4d 69 41 7a 4c 6a 49 77 4e 43 30 78 4f 43 34 34 4d 44 55 67 4e 43 34 34 4d 44 Data Ascii: yMi4yNTQgMTYuNSAzNS41NSAzIDEzLjMwNSAyLjU5NCAyNi45NTQtMS4yMDIgNDAuOTVsLTEuMiA0LjVjLTIuNTk3IDkuNjAyLTYuNTk3IDE4LjQ1LTEyIDI2LjU1LTUuMzk4IDguMDk4LTExLjg0NyAxNS4wNTItMTkuMzQ3IDIwLjg0OC03LjUgNS44MDUtMTUuODU1IDEwLjMwNS0yNS4wNSAxMy41LTkuMiAzLjIwNC0xOC44MDUgNC44MDUgNC44MD
2022-05-27 05:41:11 UTC	298	IN	Data Raw: 6e 2d 6e 6f 74 69 63 65 20 49 45 2d 77 61 72 6e 69 6e 67 2d 68 69 64 65 22 20 73 74 79 6c 65 3d 22 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 65 6e 74 2d 77 72 61 70 70 65 72 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 64 65 74 61 69 6c 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 69 63 6f 6e 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 69 63 6f 6e 22 3e 3c 2f 73 70 61 6e 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 Data Ascii: n-notice IE-warning-hide" style="display: none"> <div class="content-wrapper"> <div id="IE-warning-detail"> <div id="IE-warning-icon-container"></div>
2022-05-27 05:41:11 UTC	306	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6c 65 61 72 22 20 69 64 3d 22 70 75 73 68 22 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 66 6f 72 6d 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2 0 20 20 20 20 20 20 3c 21 2d 2d 43 4c 4f 53 45 20 66 6f 72 6d 73 20 2d 2d 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 21 2d 2d 43 4c 4f 53 45 20 6c 6f 67 69 6e 2d 73 75 62 20 20 2d 2d 3e 0a Data Ascii: </div> <div class="clear" id="push"></div> </form> ...CLOSE forms --> </div> ...CLOSE login-sub -->
2022-05-27 05:41:11 UTC	312	IN	Data Raw: 6d 22 29 3b 76 61 72 20 73 65 74 5f 6f 70 61 63 69 74 79 3b 69 66 28 48 41 53 5f 43 53 53 5f 4f 50 41 43 49 54 59 29 7b 73 65 74 5f 6f 70 61 63 69 74 79 3d 66 75 6e 63 74 69 6f 6e 20 73 65 74 4f 70 61 63 69 74 79 28 65 6c 2c 6f 70 61 63 69 74 79 29 7b 65 6c 2e 73 74 79 6c 65 2e 6f 70 61 63 69 74 79 3d 6f 70 61 63 69 74 79 7d 7d 65 6c 73 65 7b 76 61 72 20 66 69 6c 74 65 72 5f 72 65 67 65 78 3d 2f 28 44 58 49 6d 61 67 65 54 72 61 6e 73 66 6f 72 6d 5c 2e 4d 69 63 72 6f 73 6f 66 74 5c 2e 41 6c 70 68 61 5c 28 29 5b 5e 29 5d 2a 5c 29 2f 3b 73 65 74 5f 6f 70 61 63 69 74 79 3d 66 75 6e 63 74 69 6f 6e 20 73 65 74 4f 70 61 63 69 74 79 28 65 6c 2c 6f 70 61 63 69 74 79 29 7b 76 61 72 20 66 69 6c 74 65 72 5f 74 65 78 74 3d 65 6c 2e 63 75 72 72 65 6e 74 53 74 79 6c 65 Data Ascii: m");var set_opacity;if(HAS_CSS_OPACITY){set_opacity=function setOpacity(el,opacity){el.style.opacity=opacity}}else{var filter_regex=/(DXImageTransform\.Microsoft\.Alpha\()[^)]*\)/;set_opacity=function setOpacity(el,opacity){var filter_text=el.currentStyle
2022-05-27 05:41:11 UTC	314	IN	Data Raw: 70 61 63 69 74 79 2a 28 65 6e 64 2d 6e 65 77 20 44 61 74 65 29 2f 64 75 72 61 74 69 6f 6e 5f 6d 73 3b 69 66 28 6f 70 61 63 69 74 79 3c 3d 30 29 7b 6f 70 61 63 69 74 79 3d 30 3b 63 6c 65 61 72 49 6e 74 65 72 76 61 6c 28 69 6e 74 65 72 76 61 6c 29 3b 73 74 79 6c 65 5f 6f 62 6a 2e 76 69 73 69 62 69 6c 69 74 79 3d 22 68 69 64 64 65 6e 22 7d 7d 65 6c 73 65 7b 6f 70 61 63 69 74 79 3d 73 74 61 72 74 5f 6f 70 61 63 69 74 79 2b 28 31 2d 73 74 61 72 74 5f 6f 70 61 63 69 74 79 29 2a 28 6e 65 77 20 44 61 74 65 2d 73 74 61 72 74 29 2f 64 75 72 61 74 69 6f 6e 5f 6d 73 3b 69 66 28 6f 70 61 63 69 74 79 3e 3d 31 29 7b 6f 70 61 63 69 74 79 3d 31 3b 63 6c 65 61 72 49 6e 74 65 72 76 61 6c 28 69 6e 74 65 72 76 61 6c 29 7d 7d 73 65 74 5f 6f 70 61 63 69 74 79 28 65 6c 2c 6f 70 Data Ascii: pacity*(end-new Date)/duration_ms;if(opacity<=0){opacity=0;clearInterval(interval);style_obj.visibility="hidden"}}else{opacity=start_opacity+(1-start_opacity)*(new Date-start)/duration_ms;if(opacity>=1){opacity=1;clearInterval(interval)}}set_opacity(el,op
2022-05-27 05:41:12 UTC	322	IN	Data Raw: 74 2e 72 65 6d 6f 76 65 43 68 69 6c 64 28 6d 79 66 6f 72 6d 29 7d 63 6f 6e 74 65 78 74 2e 53 75 62 6d 69 74 50 6f 73 74 3d 7b 73 75 62 6d 69 74 3a 73 75 62 6d 69 74 7d 7d 29 28 77 69 6e 64 6f 77 29 3b 0a 0a 2f 2f 6a 73 74 7a 2e 6d 69 6e 2e 6a 73 0a 2f 2a 21 20 6a 73 74 7a 20 2d 20 76 31 2e 30 2e 34 20 2d 20 32 30 31 32 2d 31 32 2d 31 38 20 2a 2f 0a 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 65 3d 22 73 22 2c 6e 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 2d 65 2e 67 65 74 54 69 6d 65 7a 6f 6e 65 4f 66 66 73 65 74 28 29 3b 72 65 74 75 72 6e 20 74 21 3d 3d 6e 75 6c 6c 3f 74 3a 30 7d 2c 72 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 76 61 72 Data Ascii: t.removeChild(myform)}context.SubmitPost={submit:submit}})(window);//jstz.min.js/*! jstz - v1.0.4 - 2012-12-18 */(function(e){var t=function(){"use strict";var e="s",n=function(e){var t=-e.getTimezoneOffset();return t!==null?t:0},r=function(e,t,n){var
2022-05-27 05:41:12 UTC	328	IN	Data Raw: 69 22 7d 2c 74 79 70 65 6f 66 20 65 78 70 6f 72 74 73 21 3d 22 75 6e 64 65 66 69 6e 65 64 22 3f 65 78 70 6f 72 74 73 2e 6a 73 74 7a 3d 74 3a 65 2e 6a 73 74 7a 3d 74 7d 29 28 74 68 69 73 29 3b 0a 2f 2f 63 70 74 69 6d 65 7a 6f 6e 65 5f 6f 70 74 69 6d 69 7a 65 64 2e 6a 73 0a 28 66 75 6e 63 74 69 6f 6e 28 77 69 6e 64 6f 77 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 4a 53 54 5a 5f 52 45 4c 41 54 49 56 45 5f 50 41 54 48 3d 22 73 68 61 72 65 64 6a 73 2f 6a 73 74 7a 2e 6d 69 6e 2e 6a 73 22 3b 76 61 72 20 54 49 4d 45 5a 4f 4e 45 5f 43 4f 4f 4b 49 45 3d 22 74 69 6d 65 7a 6f 6e 65 22 3b 76 61 72 20 43 4f 4f 4b 49 45 5f 54 49 4d 45 5a 4f 4e 45 5f 4d 49 53 4d 41 54 43 48 5f 43 4c 41 53 53 3d 22 69 66 2d 74 69 6d 65 7a 6f 6e 65 2d 63 6f 6f 6b 69 65 2d 6e Data Ascii: i"},typeof exports!="undefined"?exports.jstz=t:e.jstz=t})(this);//cptimezone_optimized.js(function(window){"use strict";var JSTZ_RELATIVE_PATH="sharedjs/jstz.min.js";var TIMEZONE_COOKIE="timezone";var COOKIE_TIMEZONE_MISMATCH_CLASS="if-timezone-cookie-n

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49856	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:13 UTC	330	OUT	GET /?locale=en HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 05:41:13 UTC	330	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:13 GMT Server: Apache Content-Type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 37824 Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: webmailsession=%3arZynwdYmgajDMd6a%2c10841453a97a6117ead87650119bd7a3; HttpOnly; path=/; port=443; secure Set-Cookie: session_locale=en; expires=Sat, 27-May-2023 05:41:13 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=443; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: imp_key=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 27-May-2023 05:41:13 GMT; path=/; port=443; secure Connection: close
2022-05-27 05:41:13 UTC	332	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 64 69 72 3d 22 6c 74 72 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f Data Ascii: <!DOCTYPE html><html lang="en" dir="ltr"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1"> <meta name="goo
2022-05-27 05:41:13 UTC	338	IN	Data Raw: 67 65 22 3e 54 68 65 20 73 79 73 74 65 6d 20 68 61 73 20 64 65 74 65 63 74 65 64 20 74 68 61 74 20 79 6f 75 20 61 72 65 20 75 73 69 6e 67 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 63 50 61 6e 65 6c 20 26 61 6d 70 3b 20 57 48 4d 20 6e 6f 20 6c 6f 6e 67 65 72 20 73 75 70 70 6f 72 74 73 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 72 65 61 64 20 74 68 65 20 3c 61 20 74 69 74 6c 65 3d 22 63 50 61 6e 65 6c 20 42 6c 6f 67 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6f 2e 63 70 61 6e 65 6c 2e 6e 65 74 2f 69 65 31 31 64 65 70 72 65 63 61 74 69 6f 6e 22 3e 63 50 61 6e 65 6c 20 42 6c 6f 67 3c 2f Data Ascii: ge">The system has detected that you are using Internet Explorer 11. cPanel & WHM no longer supports Internet Explorer 11. For more information, read the <a title="cPanel Blog" target="_blank" href="https://go.cpanel.net/ie11deprecation">cPanel Blog</
2022-05-27 05:41:13 UTC	341	IN	Data Raw: 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 22 3e 73 75 6f 6d 69 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 6c 22 3e 46 69 6c 69 70 69 6e 6f 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 Data Ascii: ="locale-cell">suomi</div> <div class="locale-cell">Filipino</div> <div class="locale-cell"><a hre
2022-05-27 05:41:13 UTC	349	IN	Data Raw: 20 20 20 20 3c 2f 73 65 6c 65 63 74 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 62 75 74 74 6f 6e 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 31 30 70 78 22 20 74 79 70 65 3d 22 73 75 62 6d 69 74 22 3e 43 68 61 6e 67 65 3c 2f 62 75 74 74 6f 6e 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 66 6f 72 6d 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 23 6d 6f 62 69 6c 65 6c 6f 63 61 6c 65 6d 65 6e 75 2c 20 23 6c 6f 63 61 6c 65 73 5f 6c 69 73 74 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 7d 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 6e 6f 73 63 72 69 70 74 Data Ascii: </select> <button style="margin-left: 10px" type="submit">Change</button> </form> <style type="text/css">#mobilelocalemenu, #locales_list {display:none}</style> </noscript

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:13 UTC	354	IN	Data Raw: 65 5f 6f 75 74 5f 69 6e 73 74 65 61 64 29 7b 65 6e 64 3d 64 75 72 61 74 69 6f 6e 5f 6d 73 2b 73 74 61 72 74 2e 67 65 74 54 69 6d 65 28 29 7d 65 6c 73 65 7b 73 74 79 6c 65 5f 6f 62 6a 2e 76 69 73 69 62 69 6c 69 74 79 3d 22 76 69 73 69 62 6c 65 22 7d 76 61 72 20 66 61 64 65 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 6f 70 61 63 69 74 79 3b 69 66 28 5f 66 61 64 65 5f 6f 75 74 5f 69 6e 73 74 65 61 64 29 7b 6f 70 61 63 69 74 79 3d 73 74 61 72 74 5f 6f 70 61 63 69 74 79 2a 28 65 6e 64 2d 6e 65 77 20 44 61 74 65 29 2f 64 75 72 61 74 69 6f 6e 5f 6d 73 3b 69 66 28 6f 70 61 63 69 74 79 3c 3d 30 29 7b 6f 70 61 63 69 74 79 3d 30 3b 63 6c 65 61 72 49 6e 74 65 72 76 61 6c 28 69 6e 74 65 72 76 61 6c 29 3b 73 74 79 6c 65 5f 6f 62 6a 2e 76 69 73 69 62 69 6c 69 74 Data Ascii: e_out_instead){end=duration_ms+start.getTime()}else{style_obj.visibility="visible"}var fader=function(){var opacity;if(_fade_out_instead){opacity=start_opacity*(end-new Date)/duration_ms;if(opacity<=0){opacity=0;clearInterval(interval);style_obj.visibilit
2022-05-27 05:41:13 UTC	357	IN	Data Raw: 66 6f 72 6d 2e 71 75 65 72 79 53 65 6c 65 63 74 6f 72 28 22 2e 6e 6f 74 69 63 65 73 22 29 3b 66 6f 72 28 76 61 72 20 6e 3d 30 3b 6e 3c 72 65 73 75 6c 74 2e 6e 6f 74 69 63 65 73 2e 6c 65 6e 67 74 68 3b 6e 2b 2b 29 7b 76 61 72 20 6e 65 77 5f 70 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 70 22 29 3b 6e 65 77 5f 70 2e 74 65 78 74 43 6f 6e 74 65 6e 74 3d 72 65 73 75 6c 74 2e 6e 6f 74 69 63 65 73 5b 6e 5d 2e 63 6f 6e 74 65 6e 74 3b 63 6f 6e 74 61 69 6e 65 72 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 6e 65 77 5f 70 29 7d 63 6c 69 63 6b 5f 66 6f 72 6d 2e 6f 6e 73 75 62 6d 69 74 3d 72 65 64 69 72 65 63 74 6f 72 3b 66 61 64 65 5f 6f 75 74 28 6c 6f 67 69 6e 5f 66 6f 72 6d 29 3b 66 61 64 65 5f 69 6e 28 63 6c 69 63 6b 5f 66 6f 72 6d 29 7d Data Ascii: form.querySelector(".notices");for(var n=0;n<result.notices.length;n++){var new_p=document.createElement("p");new_p.textContent=result.notices[n].content;container.appendChild(new_p)}click_form.onsubmit=redirector;fade_out(login_form);fade_in(click_form)}
2022-05-27 05:41:13 UTC	365	IN	Data Raw: 2f 43 61 6d 70 6f 5f 47 72 61 6e 64 65 22 5d 2c 22 41 6d 65 72 69 63 61 2f 4d 6f 6e 74 65 76 69 64 65 6f 22 3a 5b 22 41 6d 65 72 69 63 61 2f 4d 6f 6e 74 65 76 69 64 65 6f 22 2c 22 41 6d 65 72 69 63 61 2f 53 61 6f 5f 50 61 75 6c 6f 22 5d 2c 22 41 73 69 61 2f 42 65 69 72 75 74 22 3a 5b 22 41 73 69 61 2f 42 65 69 72 75 74 22 2c 22 45 75 72 6f 70 65 2f 48 65 6c 73 69 6e 6b 69 22 2c 22 45 75 72 6f 70 65 2f 49 73 74 61 6e 62 75 6c 22 2c 22 41 73 69 61 2f 44 61 6d 61 73 63 75 73 22 2c 22 41 73 69 61 2f 4a 65 72 75 73 61 6c 65 6d 22 2c 22 41 73 69 61 2f 47 61 7a 61 22 5d 2c 22 50 61 63 69 66 69 63 2f 41 75 63 6b 6c 61 6e 64 22 3a 5b 22 50 61 63 69 66 69 63 2f 41 75 63 6b 6c 61 6e 64 22 2c 22 50 61 63 69 66 69 63 2f 46 69 6a 69 22 5d 2c 22 41 6d 65 72 69 63 61 2f Data Ascii: /Campo_Grande"],"America/Montevideo":["America/Montevideo","America/Sao_Paulo"],"Asia/Beirut":["Asia/Beirut","Europe/Helsinki","Europe/Istanbul","Asia/Damascus","Asia/Jerusalem","Asia/Gaza"],"Pacific/Auckland":["Pacific/Auckland","Pacific/Fiji"],"America/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49857	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:13 UTC	340	OUT	GET /cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/open_sans.min.css HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: style Referer: https://webmail.serendahsteel.com/?locale=en Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: webmailsession=%3arZynwdYmgajDMd6a%2c10841453a97a6117ead87650119bd7a3; session_locale=en; roundcube_cookies=enabled
2022-05-27 05:41:13 UTC	370	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:13 GMT Server: Apache Content-Type: text/css Last-Modified: Tue, 23 Mar 2021 16:37:21 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:13 GMT Content-Length: 6358 Connection: close
2022-05-27 05:41:13 UTC	370	IN	Data Raw: 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 27 4f 70 65 6e 20 53 61 6e 73 27 3b 73 72 63 3a 75 72 6c 28 2f 63 50 61 6e 65 6c 5f 6d 61 67 69 63 5f 72 65 76 69 73 69 6f 6e 5f 31 36 31 36 35 31 37 34 34 31 2f 75 6e 70 72 6f 74 65 63 74 65 64 2f 63 70 61 6e 65 6c 2f 66 6f 6e 74 73 2f 6f 70 65 6e 5f 73 61 6e 73 2f 4f 70 65 6e 53 61 6e 73 2d 42 6f 6c 64 2d 77 65 62 66 6f 6e 74 2e 65 6f 74 29 3b 73 72 63 3a 75 72 6c 28 2f 63 50 61 6e 65 6c 5f 6d 61 67 69 63 5f 72 65 76 69 73 69 6f 6e 5f 31 36 31 36 35 31 37 34 34 31 2f 75 6e 70 72 6f 74 65 63 74 65 64 2f 63 70 61 6e 65 6c 2f 66 6f 6e 74 73 2f 6f 70 65 6e 5f 73 61 6e 73 2f 4f 70 65 6e 53 61 6e 73 2d 42 6f 6c 64 2d 77 65 62 66 6f 6e 74 2e 65 6f 74 3f 23 69 65 66 69 78 29 20 66 6f 72 6d 61 Data Ascii: @font-face{font-family:'Open Sans';src:url(/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Bold-webfont.eot);src:url(/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Bold-webfont.eot?#iefix) forma

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49859	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:14 UTC	376	OUT	GET /cPanel_magic_revision_1630269605/unprotected/cpanel/style_v2_optimized.css HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: style Referer: https://webmail.serendahsteel.com/?locale=en Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: webmailsession=%3arZynwdYmgajDMd6a%2c10841453a97a6117ead87650119bd7a3; session_locale=en; roundcube_cookies=enabled
2022-05-27 05:41:14 UTC	378	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:14 GMT Server: Apache Content-Type: text/css Last-Modified: Sun, 29 Aug 2021 20:40:05 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:14 GMT Content-Length: 142431 Connection: close
2022-05-27 05:41:14 UTC	378	IN	Data Raw: 23 70 72 65 6c 6f 61 64 5f 69 6d 61 67 65 73 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 63 50 61 6e 65 6c 5f 6d 61 67 69 63 5f 72 65 76 69 73 69 6f 6e 5f 31 34 36 33 35 31 38 35 34 36 2f 75 6e 70 72 6f 74 65 63 74 65 64 2f 63 70 61 6e 65 6c 2f 69 6d 61 67 65 73 2f 6e 6f 74 69 63 65 2d 65 72 72 6f 72 2e 70 6e 67 29 2c 75 72 6c 28 2f 63 50 61 6e 65 6c 5f 6d 61 67 69 63 5f 72 65 76 69 73 69 6f 6e 5f 31 34 36 33 35 31 38 35 34 36 2f 75 6e 70 72 6f 74 65 63 74 65 64 2f 63 70 61 6e 65 6c 2f 69 6d 61 67 65 73 2f 6e 6f 74 69 63 65 2d 69 6e 66 6f 2e 70 6e 67 29 2c 75 72 6c 28 2f 63 50 61 6e 65 6c 5f 6d 61 67 69 63 5f 72 65 76 69 73 69 6f 6e 5f 31 34 36 33 35 31 38 35 34 36 2f 75 6e 70 72 6f 74 65 63 74 65 64 2f 63 70 61 6e 65 6c 2f 69 6d Data Ascii: #preload_images{background-image:url(/cPanel_magic_revision_1463518546/unprotected/cpanel/images/notice-error.png),url(/cPanel_magic_revision_1463518546/unprotected/cpanel/images/notice-info.png),url(/cPanel_magic_revision_1463518546/unprotected/cpanel/im
2022-05-27 05:41:14 UTC	386	IN	Data Raw: 68 3a 31 30 32 34 70 78 29 7b 23 75 73 65 72 66 6f 72 6d 20 69 6e 70 75 74 7b 77 69 64 74 68 3a 36 30 30 70 78 7d 7d 75 6c 2e 76 61 6c 69 64 61 74 69 6f 6e 5f 65 72 72 6f 72 73 5f 75 6c 3e 6c 69 2e 76 61 6c 69 64 61 74 69 6f 6e 5f 65 72 72 6f 72 73 5f 6c 69 7b 6d 61 78 2d 77 69 64 74 68 3a 32 36 30 70 78 7d 40 6d 65 64 69 61 28 6d 69 6e 2d 77 69 64 74 68 3a 34 38 30 70 78 29 7b 75 6c 2e 76 61 6c 69 64 61 74 69 6f 6e 5f 65 72 72 6f 72 73 5f 75 6c 3e 6c 69 2e 76 61 6c 69 64 61 74 69 6f 6e 5f 65 72 72 6f 72 73 5f 6c 69 7b 6d 61 78 2d 77 69 64 74 68 3a 33 38 36 70 78 7d 7d 40 6d 65 64 69 61 28 6d 69 6e 2d 77 69 64 74 68 3a 31 30 32 34 70 78 29 7b 75 6c 2e 76 61 6c 69 64 61 74 69 6f 6e 5f 65 72 72 6f 72 73 5f 75 6c 3e 6c 69 2e 76 61 6c 69 64 61 74 69 6f 6e 5f Data Ascii: h:1024px){#userform input{width:600px}}ul.validation_errors_ul>li.validation_errors_li{max-width:260px}@media(min-width:480px){ul.validation_errors_ul>li.validation_errors_li{max-width:386px}}@media(min-width:1024px){ul.validation_errors_ul>li.validation_
2022-05-27 05:41:14 UTC	386	IN	Data Raw: 6d 61 78 2d 77 69 64 74 68 3a 35 38 36 70 78 7d 7d 2e 69 6d 61 67 65 2d 77 72 61 70 70 65 72 2c 2e 74 65 78 74 2d 77 72 61 70 70 65 72 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 6d 69 64 64 6c 65 7d 2e 69 6d 61 67 65 2d 77 72 61 70 70 65 72 7b 6d 69 6e 2d 77 69 64 74 68 3a 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 39 30 70 78 7d 2e 62 75 74 74 6f 6e 2d 77 72 61 70 70 65 72 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 66 6c 6f 61 74 3a 6c 65 66 74 7d 2e 62 75 74 74 6f 6e 2d 77 72 61 70 70 65 72 20 62 75 74 74 6f 6e 7b 62 6f 72 64 65 72 3a 30 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 3b 70 61 Data Ascii: max-width:586px}}.image-wrapper,.text-wrapper{display:inline-block;overflow:hidden;vertical-align:middle}.image-wrapper{min-width:90px;min-height:90px}.button-wrapper{display:inline-block;float:left}.button-wrapper button{border:0;background-color:#fff;pa
2022-05-27 05:41:14 UTC	394	IN	Data Raw: 6c 6f 67 69 6e 2d 73 74 61 74 75 73 2d 69 63 6f 6e 2c 23 49 45 2d 77 61 72 6e 69 6e 67 20 2e 49 45 2d 77 61 72 6e 69 6e 67 2d 69 63 6f 6e 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 77 69 64 74 68 3a 32 37 70 78 3b 68 65 69 67 68 74 3a 32 37 70 78 7d 23 6c 6f 67 69 6e 2d 73 74 61 74 75 73 2e 65 72 72 6f 72 2d 6e 6f 74 69 63 65 20 2e 6c 6f 67 69 6e 2d 73 74 61 74 75 73 2d 69 63 6f 6e 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 63 50 61 6e 65 6c 5f 6d 61 67 69 63 5f 72 65 76 69 73 69 6f 6e 5f 31 34 36 33 35 31 38 35 34 36 2f 75 6e 70 72 6f 74 65 63 74 65 64 2f 63 70 61 6e 65 6c 2f 69 6d 61 67 65 73 2f 6e 6f 74 69 63 65 2d 65 72 72 6f 72 2e 70 6e 67 29 7d 23 6c 6f 67 69 6e 2d 73 74 61 74 75 73 2e 69 6e 66 6f 2d 6e 6f 74 69 63 65 20 Data Ascii: login-status-icon,#IE-warning .IE-warning-icon{display:block;width:27px;height:27px}#login-status.error-notice .login-status-icon{background-image:url(/cPanel_magic_revision_1463518546/unprotected/cpanel/images/notice-error.png)}#login-status.info-notice
2022-05-27 05:41:14 UTC	401	IN	Data Raw: 7d 68 74 6d 6c 5b 64 69 72 3d 22 72 74 6c 22 5d 20 23 72 65 73 65 74 5f 66 6f 72 6d 20 2e 69 6e 70 75 74 2d 67 72 6f 75 70 20 69 6e 70 75 74 2e 73 74 64 5f 74 65 78 74 62 6f 78 2c 68 74 6d 6c 5b 64 69 72 3d 22 72 74 6c 22 5d 20 2e 69 6e 70 75 74 2d 66 69 65 6c 64 2d 6c 6f 67 69 6e 2e 69 63 6f 6e 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 70 6f 73 69 74 69 6f 6e 3a 72 69 67 68 74 7d 2e 69 6e 70 75 74 2d 62 75 74 74 6f 6e 7b 77 69 64 74 68 3a 32 38 30 70 78 7d 69 6e 70 75 74 2e 73 74 64 5f 74 65 78 74 62 6f 78 7b 68 65 69 67 68 74 3a 32 39 70 78 3b 6d 69 6e 2d 77 69 64 74 68 3a 32 32 30 70 78 7d 68 74 6d 6c 5b 64 69 72 3d 22 72 74 6c 22 5d 20 23 72 65 73 65 74 5f 66 6f 72 6d 20 2e 69 6e 70 75 74 2d 67 72 6f 75 70 20 69 6e 70 75 74 2e 73 74 64 5f 74 65 78 74 62 6f Data Ascii: }html[dir="rtl"] #reset_form .input-group input.std_textbox,html[dir="rtl"] .input-field-login.icon{background-position:right}.input-button{width:280px}input.std_textbox{height:29px;min-width:220px}html[dir="rtl"] #reset_form .input-group input.std_textbo
2022-05-27 05:41:14 UTC	402	IN	Data Raw: 61 64 64 69 6e 67 3a 30 7d 23 6c 6f 63 61 6c 65 2d 63 6f 6e 74 61 69 6e 65 72 7b 77 69 64 74 68 3a 31 30 30 25 3b 68 65 69 67 68 74 3a 61 75 74 6f 3b 6d 69 6e 2d 77 69 64 74 68 3a 32 38 30 70 78 3b 6d 61 72 67 69 6e 3a 31 35 70 78 20 30 3b 63 6f 6c 6f 72 3a 23 32 39 33 61 34 61 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 4f 70 65 6e 20 53 61 6e 73 22 2c 73 61 6e 73 2d 73 65 72 69 66 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 36 30 30 3b 70 61 64 64 69 6e 67 3a 30 7d 23 6c 6f 63 61 6c 65 2d 63 6f 6e 74 61 69 6e 65 72 20 61 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 64 30 33 66 30 30 7d 23 6c 6f 63 61 6c 65 2d 6d 61 70 20 2e 73 63 72 6f 6c 6c 65 72 7b 6d 61 78 2d 68 65 69 67 68 74 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 3a 30 7d 23 6c 6f 63 61 6c 65 2d 68 65 61 64 Data Ascii: adding:0}#locale-container{width:100%;height:auto;min-width:280px;margin:15px 0;color:#293a4a;font-family:"Open Sans",sans-serif;font-weight:600;padding:0}#locale-container a:hover{color:#d03f00}#locale-map .scroller{max-height:none;padding:0}#locale-head

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:15 UTC	415	IN	Data Raw: 6f 6e 74 65 6e 74 3a 22 5c 66 30 34 32 22 7d 2e 66 61 2d 61 64 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 37 30 22 7d 2e 66 61 2d 61 64 6f 62 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 37 37 38 22 7d 2e 66 61 2d 61 64 76 65 72 73 61 6c 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 33 36 61 22 7d 2e 66 61 2d 61 66 66 69 6c 69 61 74 65 74 68 65 6d 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 33 36 62 22 7d 2e 66 61 2d 61 69 72 2d 66 72 65 73 68 65 6e 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 35 64 30 22 7d 2e 66 61 2d 61 69 72 62 6e 62 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 38 33 34 22 7d 2e 66 61 2d 61 6c 67 6f 6c 69 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 Data Ascii: ontent:"\f042"}.fa-adn:before{content:"\f170"}.fa-adobe:before{content:"\f778"}.fa-adversal:before{content:"\f36a"}.fa-affiliatetheme:before{content:"\f36b"}.fa-air-freshener:before{content:"\f5d0"}.fa-airbnb:before{content:"\f834"}.fa-algolia:before{cont
2022-05-27 05:41:15 UTC	422	IN	Data Raw: 73 71 75 61 72 65 2d 6c 65 66 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 39 31 22 7d 2e 66 61 2d 63 61 72 65 74 2d 73 71 75 61 72 65 2d 72 69 67 68 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 35 32 22 7d 2e 66 61 2d 63 61 72 65 74 2d 73 71 75 61 72 65 2d 75 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 35 31 22 7d 2e 66 61 2d 63 61 72 65 74 2d 75 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5 c 66 30 64 38 22 7d 2e 66 61 2d 63 61 72 72 6f 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 37 38 37 22 7d 2e 66 61 2d 63 61 72 74 2d 61 72 72 6f 77 2d 64 6f 77 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 31 38 22 7d 2e 66 61 2d 63 61 72 74 2d 70 6c 75 73 3a 62 65 66 6f Data Ascii: square-left:before{content:"\f191"}.fa-caret-square-right:before{content:"\f152"}.fa-caret-square-up:before{content:"\f151"}.fa-caret-up:before{content:"\f0d8"}.fa-carrot:before{content:"\f787"}.fa-cart-arrow-down:before{content:"\f218"}.fa-cart-plus:befo
2022-05-27 05:41:15 UTC	423	IN	Data Raw: 6b 2d 63 69 72 63 6c 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 35 38 22 7d 2e 66 61 2d 63 68 65 63 6b 2d 64 6f 75 62 6c 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 35 36 30 22 7d 2e 66 61 2d 63 68 65 63 6b 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 34 61 22 7d 2e 66 61 2d 63 68 65 65 73 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 37 65 66 22 7d 2e 66 61 2d 63 68 65 73 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 34 33 39 22 7d 2e 66 61 2d 63 68 65 73 73 2d 62 69 73 68 6f 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 34 33 61 22 7d 2e 66 61 2d 63 68 65 73 73 2d 62 6f 61 72 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 34 33 Data Ascii: k-circle:before{content:"\f058"}.fa-check-double:before{content:"\f560"}.fa-check-square:before{content:"\f14a"}.fa-cheese:before{content:"\f7ef"}.fa-chess:before{content:"\f439"}.fa-chess-bishop:before{content:"\f43a"}.fa-chess-board:before{content:"\f43
2022-05-27 05:41:15 UTC	431	IN	Data Raw: 6e 74 3a 22 5c 66 30 34 39 22 7d 2e 66 61 2d 66 61 73 74 2d 66 6f 72 77 61 72 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 35 30 22 7d 2e 66 61 2d 66 61 78 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 61 63 22 7d 2e 66 61 2d 66 65 61 74 68 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 35 32 64 22 7d 2e 66 61 2d 66 65 61 74 68 65 72 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 35 36 62 22 7d 2e 66 61 2d 66 65 64 65 78 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 37 39 37 22 7d 2e 66 61 2d 66 6 65 64 6f 72 61 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 37 39 38 22 7d 2e 66 61 2d 66 65 6d 61 6c 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 38 32 Data Ascii: nt:"\f049"}.fa-fast-forward:before{content:"\f050"}.fa-fax:before{content:"\f1ac"}.fa-feather:before{content:"\f52d"}.fa-feather-alt:before{content:"\f56b"}.fa-fedex:before{content:"\f797"}.fa-fedora:before{content:"\f798"}.fa-female:before{content:"\f182
2022-05-27 05:41:15 UTC	438	IN	Data Raw: 74 65 6e 74 3a 22 5c 66 32 35 37 22 7d 2e 66 61 2d 68 61 6e 64 2d 73 70 6f 63 6b 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 35 39 22 7d 2e 66 61 2d 68 61 6e 64 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 34 63 32 22 7d 2e 66 61 2d 68 61 6e 64 73 2d 68 65 6c 70 69 6e 67 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 34 63 34 22 7d 2e 66 61 2d 68 61 6e 64 73 68 61 6b 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3 a 22 5c 66 32 62 35 22 7d 2e 66 61 2d 68 61 6e 75 6b 69 61 68 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 36 65 36 22 7d 2e 66 61 2d 68 61 72 64 2d 68 61 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 38 30 37 22 7d 2e 66 61 2d 68 61 73 68 74 61 67 3a 62 65 66 6f 72 65 7b 63 6f Data Ascii: tent:"\f257"}.fa-hand-spock:before{content:"\f259"}.fa-hands:before{content:"\f4c2"}.fa-hands-helping:before{content:"\f4c4"}.fa-handshake:before{content:"\f2b5"}.fa-hanukiah:before{content:"\f6e6"}.fa-hard-hat:before{content:"\f807"}.fa-hashtag:before{co
2022-05-27 05:41:15 UTC	439	IN	Data Raw: 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 35 32 22 7d 2e 66 61 2d 68 6f 75 72 67 6c 61 73 73 2d 73 74 61 72 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 35 31 22 7d 2e 66 61 2d 68 6f 75 73 65 2d 64 61 6d 61 67 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 36 66 31 22 7d 2e 66 61 2d 68 6f 75 7a 7a 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 37 63 22 7d 2e 66 61 2d 68 72 79 76 6e 69 61 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 36 36 32 22 7d 2e 66 61 2d 68 74 6d 6c 35 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 33 62 22 7d 2e 66 61 2d 68 75 62 73 70 6f 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 33 62 32 22 7d 2e 66 61 2d 69 2d 63 75 72 73 6f 72 3a 62 65 66 6f 72 65 7b Data Ascii: content:"\f252"}.fa-hourglass-start:before{content:"\f251"}.fa-house-damage:before{content:"\f6f1"}.fa-houzz:before{content:"\f27c"}.fa-hryvnia:before{content:"\f6f2"}.fa-html5:before{content:"\f13b"}.fa-hubspot:before{content:"\f3b2"}.fa-i-cursor:before{
2022-05-27 05:41:15 UTC	447	IN	Data Raw: 31 62 30 22 7d 2e 66 61 2d 70 61 79 70 61 6c 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 65 64 22 7d 2e 66 61 2d 70 65 61 63 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 36 37 63 22 7d 2e 66 61 2d 70 65 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 33 30 34 22 7d 2e 66 61 2d 70 65 6e 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 33 30 35 22 7d 2e 66 61 2d 70 65 6e 2d 66 61 6e 63 79 3a 62 6 5 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 35 61 63 22 7d 2e 66 61 2d 70 65 6e 2d 6e 69 62 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 35 61 64 22 7d 2e 66 61 2d 70 65 6e 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 34 62 22 7d 2e 66 61 2d 70 65 6e Data Ascii: 1b0"}.fa-paypal:before{content:"\f1ed"}.fa-peace:before{content:"\f67c"}.fa-pen:before{content:"\f304"}.fa-pen-alt:before{content:"\f305"}.fa-pen-fancy:before{content:"\f5ac"}.fa-pen-nib:before{content:"\f5ad"}.fa-pen-square:before{content:"\f14b"}.fa-pen
2022-05-27 05:41:15 UTC	453	IN	Data Raw: 61 22 7d 2e 66 61 2d 73 68 6f 70 77 61 72 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 35 62 35 22 7d 2e 66 61 2d 73 68 6f 77 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 63 63 22 7d 2e 66 61 2d 73 68 75 74 74 6c 65 2d 76 61 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 35 62 36 22 7d 2e 66 61 2d 73 69 67 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 34 64 39 22 7d 2e 66 61 2d 73 69 67 6e 2d 6 9 6e 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 66 36 22 7d 2e 66 61 2d 73 69 67 6e 2d 6c 61 6e 67 75 61 67 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 61 37 22 7d 2e 66 61 2d 73 69 67 6e 2d 6f 75 74 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 Data Ascii: a"}.fa-shopware:before{content:"\f5b5"}.fa-shower:before{content:"\f2cc"}.fa-shuttle-van:before{content:"\f5b6"}.fa-sign:before{content:"\f4d9"}.fa-sign-in-alt:before{content:"\f2f6"}.fa-sign-language:before{content:"\f2a7"}.fa-sign-out-alt:before{content

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:15 UTC	455	IN	Data Raw: 74 2d 75 70 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 38 38 35 22 7d 2e 66 61 2d 73 6f 72 74 2d 64 6f 77 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 64 64 22 7d 2e 66 61 2d 73 6f 72 74 2d 6e 75 6d 65 72 69 63 2d 64 6f 77 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 36 32 22 7d 2e 66 61 2d 73 6f 72 74 2d 6e 75 6d 65 72 69 63 2d 64 6f 77 6e 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 38 38 36 22 7d 2e 66 61 2d 73 6f 72 74 2d 6e 75 6d 65 72 69 63 2d 75 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 36 33 22 7d 2e 66 61 2d 73 6f 72 74 2d 6e 75 6d 65 72 69 63 2d 75 70 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 38 38 37 22 7d 2e 66 Data Ascii: t-up-alt:before{content:"\f885"}.fa-sort-down:before{content:"\f0dd"}.fa-sort-numeric-down:before{content:"\f162"}.fa-sort-numeric-down-alt:before{content:"\f886"}.fa-sort-numeric-up:before{content:"\f163"}.fa-sort-numeric-up-alt:before{content:"\f887"}.f
2022-05-27 05:41:15 UTC	463	IN	Data Raw: 61 2d 76 69 62 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 34 30 39 22 7d 2e 66 61 2d 76 69 64 65 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 33 64 22 7d 2e 66 61 2d 76 69 64 65 6f 2d 73 6c 61 73 68 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 34 65 32 22 7d 2e 66 61 2d 76 69 68 61 72 61 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 36 61 37 22 7d 2e 66 61 2d 76 69 6d 65 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 34 30 61 22 7d 2e 66 61 2d 76 69 6d 65 6f 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 39 34 22 7d 2e 66 61 2d 76 69 6d 65 6f 2d 76 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 37 64 22 7d 2e 66 61 2d 76 69 6e 65 3a 62 Data Ascii: a-viber:before{content:"\f409"}.fa-video:before{content:"\f03d"}.fa-video-slash:before{content:"\f4e2"}.fa-vihara:before{content:"\f6a7"}.fa-vimeo:before{content:"\f40a"}.fa-vimeo-square:before{content:"\f194"}.fa-vimeo-v:before{content:"\f27d"}.fa-vine:b
2022-05-27 05:41:15 UTC	469	IN	Data Raw: 6e 67 74 68 2d 32 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 30 7d 75 6c 2e 73 74 72 65 6e 67 74 68 20 2e 73 74 72 65 6e 67 74 68 2d 33 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 39 66 30 7d 75 6c 2e 73 74 72 65 6e 67 74 68 20 2e 73 74 72 65 6e 67 74 68 2d 34 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 30 66 30 7d 2e 67 72 6f 77 6c 2d 63 6f 6e 74 61 69 6e 65 72 2e 67 72 6f 77 6c 2d 66 69 78 65 64 2e 74 6f 70 2d 72 69 67 68 74 3a 3b 66 6c 6f 61 74 3a 72 69 67 68 74 3b 77 69 64 74 68 3a 33 30 25 3b 6d 61 78 2d 77 69 64 74 68 3a 34 30 30 70 78 3b 7a 2d 69 6e 64 65 78 3a 39 39 39 39 7d 2e 67 72 6f 77 6c 2d 63 6f 6e 74 61 69 6e 65 72 2e 67 72 6f 77 6c 2d 66 69 78 65 64 2e 74 6f 70 2d 72 69 67 68 74 7b Data Ascii: ngth-2{background-color:#ff0}ul.strength .strength-3{background-color:#9f0}ul.strength .strength-4{background-color:#0f0}.growl-container.growl-fixed{position:fixed;float:right;width:90%;max-width:400px;z-index:9999}.growl-container.growl-fixed.top-right{
2022-05-27 05:41:15 UTC	471	IN	Data Raw: 48 43 41 41 41 52 4b 43 42 4b 72 42 42 47 2f 54 42 47 43 7a 41 42 68 7a 42 42 64 7a 42 43 2f 78 67 4e 6f 52 43 4a 4d 54 43 51 68 42 43 43 6d 53 41 48 48 4a 67 4b 61 79 43 51 69 69 47 7a 62 41 64 4b 6d 41 76 31 45 41 64 4e 4d 42 52 61 49 61 54 63 41 34 75 77 6c 57 34 44 6a 31 77 44 2f 70 68 43 4a 37 42 4b 4c 79 42 43 51 52 42 79 41 67 54 59 53 48 61 69 41 46 69 69 6c 67 6a 6a 67 67 58 6d 59 58 34 49 63 46 49 42 42 4b 4c 4a 43 44 4a 69 42 52 52 49 6b 75 52 4e 55 67 78 55 6f 70 55 49 46 56 49 48 66 49 39 63 67 49 35 68 31 78 47 75 70 45 37 79 41 41 79 67 76 79 47 76 45 63 78 6c 49 47 79 55 54 33 55 44 4c 56 44 75 61 67 33 47 6f 52 47 6f 67 76 51 5a 48 51 78 6d 6f 38 57 6f 4a 76 51 63 72 51 61 50 59 77 32 6f 65 66 51 71 32 67 50 32 6f 38 2b 51 38 63 77 77 4f Data Ascii: HCAAARKCBKrBBG/TBGCzABhzBBdzBC/xgNoRCJMTCQhBCCmSAHHJgKayCQiiGzbAdKmAv1EAdNMBRaIaTcA4uwlW4Dj1wD/phCJ7BKLyBCQRByAgTYSHaiAFiilgjjggXmYX4IcFIBBKLJCDJiBRRIkuRNUgxUopUIFVIHfl9cgI5h1xGupE7yAAygvyGvEcxlIGyUT3UDLVDuag3GoRGogvQZHQxmo8WoJvQcrQaPYw2oefQq2gP2o8+Q8cwwO
2022-05-27 05:41:15 UTC	479	IN	Data Raw: 38 7a 71 68 71 73 63 30 6d 69 65 5a 4f 62 2b 62 66 68 77 61 6d 76 32 31 73 48 44 6c 58 37 35 2f 76 63 55 53 75 44 77 2b 66 6a 72 64 54 62 4f 69 56 52 6b 4d 39 39 49 6c 66 68 4a 4a 55 52 53 30 44 51 32 33 44 2f 57 69 74 43 78 4f 70 37 66 55 61 76 31 79 31 4f 62 69 6d 70 71 51 71 62 33 39 6c 63 46 6d 2b 79 4c 44 4d 4f 34 6f 6d 2f 4c 57 31 6d 57 4c 79 37 57 63 46 77 41 41 6f 4b 36 73 76 4b 62 55 36 39 6e 63 79 4d 70 61 57 73 35 64 47 42 6a 6f 74 51 38 50 4e 78 74 73 74 76 65 35 2b 7a 43 4e 4a 6b 6b 59 6a 62 65 4f 37 4b 5a 38 6d 5a 33 4f 6e 51 71 37 2f 57 46 57 35 53 59 53 77 46 42 55 4e 77 44 41 39 2b 6c 70 4d 72 71 31 64 5a 36 2f 72 69 44 4a 6c 4b 6d 74 37 62 72 5a 36 64 77 35 64 4f 6e 35 6e 73 78 50 49 79 4f 76 4e 32 64 6e 62 32 53 56 76 31 37 50 4d 70 47 Data Ascii: 8zqhqsc0miеZOb+bfhwamv21sHDlX75/vcUSuDw+fjrdTbOiVRkM99IlfhJJURS0DQ23D/WitCxOp7fUav1y1ObimpqQqb39lcFm+yLDMO4om/LW1mWLy7WcFwAAoK6svKbU69ncyMpaWs5dGBjotQ8PNxtstve5+zCNJkkYjbeO7KZ8mZ3OnQq7/WFW5SYSwFBUNwDA9+lpMrq1dZ6/riDJlKmt7brZ6dw5dOn5nsxPlyOvN2dnb2SVv17PMpG
2022-05-27 05:41:15 UTC	485	IN	Data Raw: 68 64 59 77 50 32 53 79 63 51 57 48 54 41 34 76 63 41 41 50 4b 37 62 38 48 55 4b 41 67 44 67 47 69 44 34 63 39 33 2f 2b 38 2f 55 65 67 4a 51 43 41 5a 6b 6d 53 63 51 41 41 58 6b 51 6b 4c 6c 54 4b 73 7a 2f 48 43 41 41 41 52 4b 43 42 4b 72 42 42 47 2f 54 42 47 43 7a 41 42 68 7a 42 42 64 7a 42 43 2f 78 67 4e 6f 52 43 4a 4d 54 43 51 68 42 43 43 6d 53 41 48 48 4a 67 4b 61 79 43 51 69 69 47 7a 62 41 64 4b 6d 41 76 31 45 41 64 4e 4d 42 52 61 49 61 54 63 41 34 75 77 6c 57 34 44 6a 31 77 44 2f 70 68 43 4a 37 42 4b 4c 79 42 43 51 52 42 79 41 67 54 59 53 48 61 69 41 46 69 69 6c 67 6a 6a 67 67 58 6d 59 58 34 49 63 46 49 42 42 4b 4c 4a 43 44 4a 69 42 52 52 49 6b 75 52 4e 55 67 78 55 6f 70 55 49 46 56 49 48 66 49 39 63 67 49 35 68 31 78 47 75 70 45 37 79 41 41 79 67 76 Data Ascii: hdYwP2SycQWHTA4vcAAPK7b8HUKAgDgGiD4c93/+8/UegJQCAZkmScQAAXkQkLlTKsz/HCAAARKCBKrBBG/TBGCzABhzBBdzBC/xgNoRCJMTCQhBCCmSAHHJgKayCQiiGzbAdKmAv1EAdNMBRaIaTcA4uwlW4Dj1wD/phCJ7BKLyBCQRByAgTYSHaiAFiilgjjggXmYX4IcFIBBKLJCDJiBRRIkuRNUgxUopUIFVIHfl9cgI5h1xGupE7yAAygv
2022-05-27 05:41:15 UTC	487	IN	Data Raw: 37 30 56 76 76 74 77 58 66 63 64 78 33 76 6f 39 38 50 54 2b 52 38 49 48 38 6f 2f 32 6a 35 73 66 56 54 30 4b 66 37 6b 78 6d 54 6b 2f 38 45 41 35 6a 7a 2f 47 4d 7a 4c 64 73 41 41 41 41 67 59 30 68 53 54 51 41 41 65 69 55 41 41 49 43 44 41 41 44 35 2f 77 41 41 67 4f 6b 41 41 48 55 77 41 41 44 71 59 41 41 41 4f 70 67 41 41 42 64 76 6b 6c 2f 46 52 67 41 41 41 64 68 4a 52 45 46 55 65 4e 72 55 6c 72 39 4c 49 30 45 55 78 7a 39 52 69 78 52 58 57 4f 62 51 77 73 4b 41 64 68 4a 6b 73 41 6a 59 57 6c 70 61 65 42 67 59 41 79 63 69 4b 43 68 33 42 7a 72 43 67 4d 52 66 34 46 6d 6c 38 41 62 73 39 4f 44 2b 67 65 75 30 6b 31 47 49 6e 51 63 70 7a 69 4c 43 46 58 74 67 6b 57 4b 4c 51 43 78 38 51 74 6a 4c 48 71 74 47 30 41 66 44 73 75 2f 74 7a 4a 76 76 39 2f 76 65 7a 4b 61 61 7a Data Ascii: 70VvvtwXfcdx3vo98PT+R8IH8o/2j5sfVT0Kf7kxmTk/8EA5jz/GMzLdsAAAAgY0hSTQAAeiUAAICDAAD5/wAAgOkAAHUwAADqYAAAOpgAABdvkl/FRgAAAdhJREFUeNrUlr9LI0EUxz9RixRXWObQwsKAdhJksAjYWlpaeBgYAyciKCh3BzrCgMRf4FmlI8Abs9OD+qeu0k1GInQcpziLCFXtgkWKLQCx8QtjLHqtG0AfDsu/tzJvv9/vezKaaz
2022-05-27 05:41:15 UTC	495	IN	Data Raw: 6c 65 72 74 2d 64 61 6e 67 65 72 20 2e 61 6c 65 72 74 2d 6d 65 73 73 61 67 65 20 75 6c 20 6c 69 3e 2a 7b 63 6f 6c 6f 72 3a 23 33 33 33 7d 2e 61 6c 65 72 74 20 2e 62 74 6e 2d 6d 6f 72 65 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 30 7d 5b 64 69 72 3d 22 6c 74 72 22 5d 20 62 6f 64 79 2e 77 68 6f 73 74 6d 67 72 20 2e 61 6c 65 72 74 2d 6c 69 73 74 20 2e 61 6c 65 72 74 2d 6d 65 73 73 61 67 65 2c 5b 64 69 72 3d 22 72 74 6c 22 5d 20 62 6f 64 79 2e 77 68 6f 73 74 6d 67 72 20 2e 61 6c 65 72 74 2d 6c 69 73 74 20 2e 61 6c 65 72 74 2d 6d 65 73 73 61 67 65 7b 6d 61 72 67 69 6e 3a 30 7d 5b 64 69 72 3d 22 6c 74 72 22 5d 20 62 6f 64 79 2e 77 68 6f 73 74 6d 67 72 20 2e 61 6c 65 72 74 2d 6c 69 73 74 20 2e 61 6c 65 72 74 2d 6d 65 73 73 61 67 65 3e 2e 61 6c 65 72 74 2d 74 69 74 Data Ascii: lert-danger .alert-message ul li>*{color:#333}.alert .btn-more{padding-top:0}[dir="ltr"] body.whostmgr .alert-list .alert-message,[dir="rtl"] body.whostmgr .alert-list .alert-message{margin:0}[dir="ltr"] body.whostmgr .alert-list .alert-message>.alert-tit

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:15 UTC	500	IN	Data Raw: 65 72 74 2d 6c 69 73 74 2d 63 6f 6e 74 61 69 6e 65 72 2e 70 6f 73 69 74 69 6f 6e 2d 74 6f 70 2d 6d 69 64 64 6c 65 2e 73 68 6f 77 2d 73 63 72 6f 6c 6c 2d 62 61 72 7b 6f 76 65 72 66 6c 6f 77 2d 79 3a 73 63 72 6f 6c 6c 7d 2e 77 68 6f 73 74 6d 67 72 20 2e 61 6c 65 72 74 2d 6c 69 73 74 2d 63 6f 6e 74 61 69 6e 65 72 2e 70 6f 73 69 74 69 6f 6e 2d 74 6f 70 2d 6d 69 64 64 6c 65 7b 74 6f 70 3a 37 30 70 78 7d 2e 63 70 61 6e 65 6c 5f 62 6f 64 79 20 2e 61 6c 65 72 74 2d 6c 69 73 74 2d 63 6f 6e 74 61 69 6e 65 72 2e 70 6f 73 69 74 69 6f 6e 2d 74 6f 70 2d 6d 69 64 64 6c 65 7b 74 6f 70 3a 33 30 70 78 7d 2e 77 65 62 6d 61 69 6c 20 2e 61 6c 65 72 74 2d 6c 69 73 74 2d 63 6f 6e 74 61 69 6e 65 72 2e 70 6f 73 69 74 69 6f 6e 2d 74 6f 70 2d 6d 69 64 64 6c 65 7b 74 6f 70 3a 35 32 Data Ascii: ert-list-container.position-top-middle.show-scroll-bar{overflow-y:scroll}.whostmgr .alert-list-container.position-top-middle{top:70px}.cpanel_body .alert-list-container.position-top-middle{top:30px}.webmail .alert-list-container.position-top-middle{top:52
2022-05-27 05:41:15 UTC	503	IN	Data Raw: 74 2d 6c 69 73 74 7b 77 69 64 74 68 3a 31 30 30 25 7d 40 6d 65 64 69 61 28 6d 69 6e 2d 77 69 64 74 68 3a 37 36 38 70 78 29 7b 2e 61 6c 65 72 74 2d 6c 69 73 74 2d 63 6f 6e 74 61 69 6e 65 72 2e 70 6f 73 69 74 69 6f 6e 2d 6d 69 64 64 6c 65 2d 6c 65 66 74 20 2e 61 6c 65 72 74 2d 6c 69 73 74 7b 6d 61 78 2d 77 69 64 74 68 3a 35 30 30 70 78 7d 7d 2e 61 6c 65 72 74 2d 6c 69 73 74 2d 63 6f 6e 74 61 69 6e 65 72 2e 70 6f 73 69 74 69 6f 6e 2d 6d 69 64 64 6c 65 2d 6c 65 66 74 2e 73 68 6f 77 2d 73 63 72 6f 6c 6c 2d 62 61 72 7b 6f 76 65 72 66 6c 6f 77 2d 79 3a 73 63 72 6f 6c 6c 7d 2e 61 6c 65 72 74 2d 6c 69 73 74 2d 63 6f 6e 74 61 69 6e 65 72 2e 70 6f 73 69 74 69 6f 6e 2d 6d 69 64 64 6c 65 2d 6c 65 66 74 20 2e 61 6c 65 72 74 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 31 70 78 Data Ascii: t-list{width:100%}@media(min-width:768px){.alert-list-container.position-middle-left .alert-list{max-width:500px}}.alert-list-container.position-middle-left.show-scroll-bar{overflow-y:scroll}.alert-list-container.position-middle-left .alert{margin-top:1px
2022-05-27 05:41:15 UTC	511	IN	Data Raw: 6d 61 74 65 20 2a 7b 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 69 74 69 6f 6e 3a 6e 6f 6e 65 21 69 6d 70 6f 72 74 61 6e 74 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 6e 6f 6e 65 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 75 73 65 72 2d 64 6f 6d 61 69 6e 2d 6c 69 73 74 2d 64 69 72 65 63 74 69 76 65 20 2e 6e 6f 2d 72 65 73 75 6c 74 73 2d 6d 73 67 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 7d 2e 75 73 65 72 2d 64 6f 6d 61 69 6e 2d 6c 69 73 74 2d 64 69 72 65 63 74 69 76 65 20 2e 66 69 78 65 64 2d 77 69 64 74 68 2d 74 61 62 6c 65 7b 74 61 62 6c 65 2d 6c 61 79 6f 75 74 3a 66 69 78 65 64 7d 2e 75 73 65 72 2d 64 6f 6d 61 69 6e 2d 6c 69 73 74 2d 64 69 72 65 63 74 69 76 65 20 2e 65 64 69 74 2d 6c 6f 63 6b 65 64 7b 66 6f 6e 74 2d 73 74 79 6c 65 3a 69 74 61 6c 69 63 3b 70 6f 69 6e 74 Data Ascii: mate *{-webkit-transition:none!important;transition:none!important}.user-domain-list-directive .no-results-msg{margin-top:0}.user-domain-list-directive .fixed-width-table{table-layout:fixed}.user-domain-list-directive .edit-locked{font-style:italic;pointe
2022-05-27 05:41:15 UTC	516	IN	Data Raw: 69 64 20 23 64 64 64 7d 2e 73 74 61 74 73 2d 77 69 64 67 65 74 20 68 74 6d 6c 5b 64 69 72 3d 22 72 74 6c 22 5d 20 2e 73 74 61 74 73 2d 77 69 64 67 65 74 2d 66 6f 6f 74 65 72 20 61 3a 6e 6f 74 28 3a 66 69 72 73 74 2d 63 68 69 6c 64 29 7b 62 6f 72 64 65 72 2d 72 69 67 68 74 3a 31 70 78 20 73 6f 6c 69 64 20 23 64 64 64 7d 68 74 6d 6c 5b 64 61 74 61 2d 73 74 79 6c 65 3d 22 64 61 72 6b 22 5d 20 2e 73 74 61 74 73 2d 77 69 64 67 65 74 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 32 32 32 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 3b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 31 64 31 64 31 64 3b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 33 70 78 7d 68 74 6d 6c 5b 64 61 74 61 2d 73 74 79 Data Ascii: id #ddd}.stats-widget html[dir="rtl"] .stats-widget-footer a:not(:first-child){border-right:1px solid #ddd}html[data-style="dark"] .stats-widget{background-color:#222;margin-top:20px;box-shadow:none;border:1px solid #1d1d1d;border-radius:3px}html[data-sty
2022-05-27 05:41:15 UTC	519	IN	Data Raw: 70 61 6e 65 6c 2f 69 6d 61 67 65 73 2f 69 63 6f 6e 2d 70 61 73 73 77 6f 72 64 2e 70 6e 67 29 3b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 68 65 69 67 68 74 3a 33 34 70 78 3b 77 69 64 74 68 3a 31 30 30 25 3b 6d 61 72 67 69 6e 3a 30 7d 23 72 65 73 65 74 5f 66 6f 72 6d 20 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 62 74 6e 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 77 69 64 74 68 3a 31 30 30 25 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 64 64 64 3b 62 6f 72 64 65 72 3a 32 70 78 20 73 6f 6c 69 64 20 23 62 65 62 65 62 65 3b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 30 20 30 20 34 70 78 20 34 70 78 3b 62 6f 72 64 65 72 2d 74 Data Ascii: panel/images/icon-password.png);box-sizing:border-box;height:34px;width:100%;margin:0}#reset_form .input-group-btn{box-sizing:border-box;display:block;width:100%;text-align:center;background:#ddd;border:2px solid #bebebe;border-radius:0 0 4px 4px;border-t

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49860	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:14 UTC	377	OUT	GET /cPanel_magic_revision_1463518546/unprotected/cpanel/images/webmail-logo.svg HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://webmail.serendahsteel.com/?locale=en Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: webmailsession=%3arZynwdYmgajDMd6a%2c10841453a97a6117ead87650119bd7a3; session_locale=en; roundcube_cookies=enabled
2022-05-27 05:41:14 UTC	410	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:14 GMT Server: Apache Content-Type: image/svg+xml Last-Modified: Tue, 17 May 2016 20:55:46 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:14 GMT Content-Length: 5360 Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:14 UTC	410	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 34 36 32 70 74 22 20 68 65 69 67 68 74 3d 22 33 32 30 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 34 36 32 20 32 34 30 22 3e 3c 64 65 66 73 3e 3c 63 6c 69 70 50 61 74 68 20 69 64 3d 22 61 22 3e 3c 70 61 74 68 20 64 3d 22 4d 31 33 33 39 20 30 68 31 32 32 2e 34 34 76 32 34 30 48 31 33 33 39 7a 6d 30 20 30 22 2f 3e 3c 2f 63 6c 69 70 50 61 74 68 3e 3c 2f 64 65 66 73 3e 3c 70 61 74 68 20 64 3d 22 4d 33 36 35 2e 31 30 32 20 31 34 2e 33 39 38 6c 2d 34 33 2e 32 30 34 20 31 36 30 2e 32 30 34 63 2d 32 2e 35 39 37 20 39 2e 35 39 37 2d 36 2e 35 39 37 20 31 38 2e 34 35 2d 31 32 20 32 36 2e 35 34 36 2d 35 2e 33 39 38 20 38 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="1462pt" height="320" viewBox="0 0 1462 240"><defs><clipPath id="a"><path d="M1339 0h122.44v240H1339zm0 0"/></clipPath></defs><path d="M365.102 14.398l-43.204 160.204c-2.597 9.597-6.597 18.45-12 26.546-5.398 8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49862	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:15 UTC	522	OUT	GET /cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Regular-webfont.woff HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Origin: https://webmail.serendahsteel.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: font Referer: https://webmail.serendahsteel.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/open_sans.min.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: webmailsession=%3arZynwdYmgajDMd6a%2c10841453a97a6117ead87650119bd7a3; session_locale=en; roundcube_cookies=enabled; timezone=America/Los_Angeles
2022-05-27 05:41:16 UTC	527	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:16 GMT Server: Apache Content-Type: application/font-woff Last-Modified: Tue, 23 Mar 2021 16:37:21 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:16 GMT Content-Length: 22660 Connection: close
2022-05-27 05:41:16 UTC	527	IN	Data Raw: 77 4f 46 46 00 01 00 00 00 00 58 84 00 13 00 00 00 00 95 58 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 46 46 54 4d 00 00 01 a8 00 00 00 1c 00 00 00 1c 63 47 ec 8f 47 44 45 46 00 00 01 c4 00 00 00 1e 00 00 00 20 01 1d 00 04 47 50 4f 53 00 00 01 e4 00 00 04 a3 00 00 09 9e 2d 72 17 42 47 53 55 42 00 00 06 88 00 00 00 81 00 00 00 a8 a0 63 88 a1 4f 53 2f 32 00 00 07 0c 00 00 00 60 00 00 00 60 a0 e5 99 7f 63 6d 61 70 00 00 07 6c 00 00 01 a2 00 00 02 0a 13 f0 34 51 63 76 74 20 00 00 09 10 00 00 00 30 00 00 00 3c 29 c6 06 3b 66 70 67 6d 00 00 09 40 00 00 04 fa 00 00 09 91 8b 0b 7a 41 67 61 73 70 00 00 0e 3c 00 00 00 08 00 00 00 08 00 00 00 10 67 6c 79 66 00 00 0e 44 00 00 41 3e 00 00 6f 70 52 6a bc 2d 68 65 61 64 00 00 4f 84 00 00 00 Data Ascii: wOFFXXFFTMcGGDEF GPOS-rBGSUBcOS/2``cmapl4Qcvt 0<);fpgm@zAgasp<glyfDA>opRj-headO
2022-05-27 05:41:16 UTC	535	IN	Data Raw: fa a8 fe 1e 93 f3 e3 bf 37 9e 45 6e 55 7e 53 50 64 3c 2b 1d a7 db e9 eb 4c d9 e0 d1 10 71 74 c5 63 af 4f 0f 7e f7 9f 9f 7f fa fe 3f 41 88 6b 9f a4 f7 82 14 57 e3 09 78 39 bd 8f ee a0 17 e8 db 38 07 b7 83 d8 36 9b aa f9 6b b6 de d5 7c df da b4 9d 0b 62 84 58 f4 c7 f7 56 28 a4 4a 73 bb ad a9 3c 1d 2a ba 79 38 95 82 fd 9a 56 16 ab e9 39 fa c5 de 7a 3c 97 a4 05 a3 36 7f fa d6 f1 d3 c7 45 e3 df ff 1d 04 7a 83 09 eb 9e 5c bb 9a d3 4a 77 71 5a a3 61 57 43 e4 0b ab 26 30 8f 1f a3 c9 21 50 dc 17 09 7b e8 10 91 f0 f4 ab 85 25 c2 b0 72 73 da 3f 7d 07 8f fc 89 5e 29 b8 25 fd 5f d2 95 c5 b4 16 f7 23 bf c2 05 95 07 67 81 07 46 60 38 c4 97 7a e6 76 17 23 11 e2 28 24 0a 2c ba d4 54 b2 b6 ec b0 2e f6 68 13 8c 36 82 0e 03 6b 89 39 3f 44 a7 45 02 4c bd 21 b6 80 66 c3 6b 81 Data Ascii: 7EnU~SPd<+LqtcO~?AkWx986k|bXV(Js<*y8V9z<6Ez\JwqZaWC&0!P{%rs?}^)%_#gF`8zv#($,T.h6k9?DEL!fk
2022-05-27 05:41:16 UTC	555	IN	Data Raw: d0 3b 67 e9 df 27 06 a7 90 d1 eb d6 ac 59 fb 10 b0 81 f9 fe 04 74 5e 1a ca 0a b4 8b 05 9d 17 27 83 39 62 81 91 50 1c a1 e8 9a bd 7d 4f a6 2a 18 60 21 53 42 e1 24 b8 f3 3e 1e b6 a8 0a 8f f9 f9 49 d8 95 04 b6 9f fe e3 5b da b8 72 f8 7b d5 f5 7b bb af 59 f7 97 e7 e8 b9 bf 1d ce 3b b8 67 e9 a6 ce 8b 97 7f f1 27 bc f8 c4 87 25 bb d2 db 2f 98 3e 60 4c 79 ee 6d a7 9e 7c f6 54 d9 86 01 33 ee 1a 30 66 70 76 f9 31 be 1f 6c c0 a3 e1 c0 23 85 e5 3f 60 f5 30 4b 62 91 08 c5 ae aa 04 96 c4 72 ba c9 8a 7a 9a 2d f6 a5 d9 52 f2 c6 8d aa 5e 39 0a b2 1e 07 cf 5b 99 ce 64 29 38 f5 88 24 44 0d fc 6f 45 56 8f dd 23 31 7e 3a d8 52 73 5d a5 2a 2d 29 8e fe 95 fe 0c 7f 2f d7 9f 7a f5 c5 53 d2 a1 c6 db af d1 4f 71 4a a3 b0 af b1 f7 e1 d7 df 38 22 1c 61 30 e0 8f f8 5a 38 47 c3 c2 83 Data Ascii: ;g'Yt^'9bP}O*`!SB$>l[r{{Y;g'%/>`Lym|T30fpv1l#?`0Kbrz-R^9[d)8$DoEV#1~:Rs]*-)/zSOqJ8"a0Z8G
2022-05-27 05:41:16 UTC	563	IN	Data Raw: 90 cb d7 07 88 07 0e fc 79 bb aa 8f 78 0f 83 ec 66 eb 3a 8a ad 2b bb 34 40 46 25 ab 11 7a 2a 10 dd b1 1d d1 e9 ed 10 c3 da b4 d3 a5 38 1e b5 ea f4 a2 5e 27 56 df d0 b3 a0 d7 9b 4b 9a 1b 17 a2 78 0d b8 21 dc e3 90 8f f4 3a 7d 0d d2 89 ba 9a 5b 77 3b 18 78 b7 43 54 8b 6e 87 b8 36 09 18 b7 cf f4 a5 43 cc ee 6d e3 c5 f1 38 9e 75 3c d8 8c c9 99 bf 46 c3 ac 4c 4e 43 66 3a d1 eb 6e a4 01 08 00 32 6e a4 41 a7 fb 75 1a 74 7a 40 1f e8 ff bf d0 d0 b1 43 bb 8c ff 1d 0d 27 3f 44 68 77 c0 92 9d 95 2e dc 48 44 be 01 ff 3e 2a 8c 1c 95 a8 30 15 05 9c 0a 78 fa 57 c9 88 e2 64 18 5b 90 91 c0 c8 c8 f5 df 84 10 53 72 66 33 1d d2 c7 ad e8 38 f5 12 42 2f 05 0c 21 0a 42 1d 32 dd c3 d0 8d 06 0b d1 89 46 dd 88 08 61 8a aa 30 e1 a8 28 47 04 21 d1 1c 19 73 98 90 9e ff cb e7 cd 9c a4 Data Ascii: yxf:+4@F%z*8^'VKx!:}[w;xCTn6Cm8u<FLNCf:n2nAutz@C'?Dhw.HD>*0xWd[Srf38B/!B2Fa0(G!s

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49861	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:16 UTC	523	OUT	GET /cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Semibold-webfont.woff HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Origin: https://webmail.serendahsteel.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: font Referer: https://webmail.serendahsteel.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/open_sans.min.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: webmailsession=%3arZynwdYmgajDMd6a%2c10841453a97a6117ead87650119bd7a3; session_locale=en; roundcube_cookies=enabled; timezone=America/Los_Angeles
2022-05-27 05:41:16 UTC	535	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:16 GMT Server: Apache Content-Type: application/font-woff Last-Modified: Tue, 23 Mar 2021 16:37:21 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:16 GMT Content-Length: 22908 Connection: close
2022-05-27 05:41:16 UTC	535	IN	Data Raw: 77 4f 46 46 00 01 00 00 00 00 59 7c 00 13 00 00 00 00 9a 34 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 46 46 54 4d 00 00 01 a8 00 00 00 1c 00 00 00 1c 63 5f a5 d6 47 44 45 46 00 00 01 c4 00 00 00 1e 00 00 00 20 01 1c 00 04 47 50 4f 53 00 00 01 e4 00 00 04 a3 00 00 09 9e 2d 72 17 42 47 53 55 42 00 00 06 88 00 00 00 81 00 00 00 a8 a0 62 88 9e 4f 53 2f 32 00 00 07 0c 00 00 00 5f 00 00 00 60 a1 cc 92 87 63 6d 61 70 00 00 07 6c 00 00 01 9c 00 00 02 02 b7 6f 6c be 63 76 74 20 00 00 09 08 00 00 00 30 00 00 00 3c 2a 72 06 89 66 70 67 6d 00 00 09 38 00 00 04 fa 00 00 09 91 8b 0b 7a 41 67 61 73 70 00 00 0e 34 00 00 00 08 00 00 00 08 00 00 00 10 67 6c 79 66 00 00 0e 3c 00 00 42 2a 00 00 73 e8 80 99 2f ad 68 65 61 64 00 00 50 68 00 00 00 Data Ascii: wOFFY|4FFTMc_GDEF GPOS-rBGSUBbOS/2_`cmaplolcvt 0<*rfpgm8zAgasp4glyf<B*s/headPh
2022-05-27 05:41:16 UTC	543	IN	Data Raw: 42 e3 5d e5 04 5b cf 5e 61 2f b3 27 d1 20 0c 82 7e 30 f1 f2 a6 4f 3e fa f0 e4 c7 1f 7e 7c 8a 9e c6 cf ee 45 ce ae c1 3f 73 d9 74 b6 8e 9d 67 df 80 13 6c 48 ba 68 f6 2d 31 74 90 bc 50 c4 bd 0e 43 92 91 b5 08 0f 09 85 ac 05 43 ad b4 54 8f 2d 55 a4 37 65 8f 08 b3 52 e4 e6 40 50 5e c8 fe ce ce ad f9 01 9e 01 3b d8 9a 32 66 ef 7e 7e dd d3 9b a5 c6 33 17 38 5b fc 93 45 3f fc c8 43 0f f2 b5 66 b2 4d 02 df 48 f4 35 da 07 32 70 0b 25 1e 05 00 b9 33 b8 9c f0 4b 9a dd c6 b4 34 8f 48 a9 46 f1 74 58 50 b6 db e2 ff ee 41 18 c3 f6 b1 86 8c eb 12 e1 22 5b 39 90 2d 80 92 df a0 84 ae 8b 2d 42 17 bb b8 dd b4 83 42 38 6c 68 b8 28 57 3d 46 ca b3 39 6b 6d 36 9b 5d 66 97 cb 63 4f e3 46 0b 5a 8c 94 20 8d 2b 4a 41 80 61 db e6 67 57 6d 7c fa a9 1f e0 49 88 47 49 f9 12 9e 64 3f b2 Data Ascii: B][^a/' ~0O>~|E?stglHh-1tPCCT-U7eR@P^;2f~~38[E?CfMH52p%3K4HFtXPA"[9--BB8lh(W=F9km6]fcOFZ +JAagWm|IGId?
2022-05-27 05:41:16 UTC	569	IN	Data Raw: 2d 11 32 33 11 ed 93 15 f5 60 1a cf 1d b8 51 0f c6 a8 54 0f 05 a4 c2 10 e5 d7 e2 f9 7b db eb cc c1 63 98 96 d0 5c 24 9d 85 61 e2 ce 88 88 60 92 a8 6c 65 67 7f f9 e5 a9 89 9f 8f 7b 6c c1 83 07 8f 6c 02 f9 d4 07 ef 0f 3e b4 f6 de fb bb 4c 5e fa e7 55 fd 60 c9 a1 cf 6e fc 57 e7 fc bb 2a cb a6 0e 29 7d 7f f9 ae 0f 46 1f 2a bb ad bc 5b 69 49 8f a2 7b 97 eb fe 68 22 f2 4a 35 d2 48 e3 39 12 dc 3d a0 a5 3a 8b 04 f5 20 57 17 5c 0b a2 43 eb a1 7b 7e 60 65 f2 20 7c 7d 73 f4 a8 3e 7e 07 f2 7b 0f 21 57 a8 4b 79 3a 4e 3f c6 08 62 83 7f db 88 cd eb 48 53 ec 59 80 ba 4b c6 1d 17 5a 2c 3a 27 25 16 94 1e 8b d8 af bb 90 80 1f fc 58 bf 15 ca 94 9d 8d 43 36 fe 54 07 29 8d d2 d6 c6 09 2f 3f 0f 13 a4 f5 7c 0d 22 ce 20 b8 be 44 18 cd 3c 4c 28 e4 e2 1a e4 63 84 51 c2 d9 73 c0 8b Data Ascii: -23`QT{c\$a`leg{ll>L^U`nW*)}F*[il{h"J5H9=: W\C{~`e |}s>~{!WKy:N?bHSYKZ,:'%XC6T)/?|" D<L(cQs
2022-05-27 05:41:16 UTC	577	IN	Data Raw: fe 94 d9 f3 cf 01 fc f0 39 3a b1 67 06 ce cb e9 db 3d 21 29 27 3d d0 fb d6 bb fb 3f f3 7c 9f b7 7c 5d 57 f7 1a 39 70 c0 83 c3 0b ee c8 f3 df 94 53 52 7a d7 1d 97 a7 c9 cb 0e 1c ad c7 bd 16 fd 10 aa 87 ef f5 28 be d7 c5 c2 f7 2e 5a 4b 48 43 20 b2 4b 16 35 9b 5c 20 c9 4e e3 74 8b 53 28 df 0a 66 93 6c 32 cb d5 57 f5 4a 98 4c 11 45 2d 5d 10 61 a2 ff c1 d2 52 20 c3 d3 79 dd 43 47 b7 6e 9f 68 3d da 22 8a 63 c2 42 7a 28 e2 03 7e 62 32 9b 6a 70 06 d9 5c 73 fd ee 8b ab 47 e2 06 24 b6 6b 97 94 08 d0 ae 6b bb ae 1d 3b 20 cf 67 24 65 40 02 24 f0 36 0c 7b 78 b2 6e 1b ae 4d 8b e9 83 05 2d 3a 65 fe ff b4 20 6f 7e 4d c8 f9 40 54 4e a7 f6 92 c9 dc 96 18 fe 70 0b 45 64 10 a5 ab a9 61 36 87 e2 63 15 f0 84 b5 a6 46 8f 56 c3 5b e3 d3 7a 78 98 40 ca da 8a 1c 37 10 b3 c9 5c c3 Data Ascii: 9:g=!)'=?|[]W9pSRz(.ZKHC K5\ NtS(fl2WJLE-]aR yCGnh="cBz(~b2jp\sG$kk; g$e@$6{xnM-:e o~M@T NpEda6cFV[zx@7\

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49863	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:16 UTC	524	OUT	GET /cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Bold-webfont.woff HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Origin: https://webmail.serendahsteel.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: font Referer: https://webmail.serendahsteel.com/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/open_sans.min.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: webmailsession=%3arZynwdYmgajDMd6a%2c10841453a97a6117ead87650119bd7a3; session_locale=en; roundcube_cookies=enabled; timezone=America/Los_Angeles
2022-05-27 05:41:16 UTC	543	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:16 GMT Server: Apache Content-Type: application/font-woff Last-Modified: Tue, 23 Mar 2021 16:37:21 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:16 GMT Content-Length: 22432 Connection: close
2022-05-27 05:41:16 UTC	544	IN	Data Raw: 77 4f 46 46 00 01 00 00 00 00 57 a0 00 13 00 00 00 00 96 34 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 46 46 54 4d 00 00 01 a8 00 00 00 1c 00 00 00 1c 63 54 d3 4e 47 44 45 46 00 00 01 c4 00 00 00 1e 00 00 00 20 01 1c 00 04 47 50 4f 53 00 00 01 e4 00 00 04 a3 00 00 09 9e 2d 72 17 42 47 53 55 42 00 00 06 88 00 00 00 81 00 00 00 a8 a0 62 88 9e 4f 53 2f 32 00 00 07 0c 00 00 00 60 00 00 00 60 a2 49 9b dd 63 6d 61 70 00 00 07 6c 00 00 01 9c 00 00 02 02 b7 6f 6c be 63 76 74 20 00 00 09 08 00 00 00 32 00 00 00 3c 2b 73 06 e0 66 70 67 6d 00 00 09 3c 00 00 04 fa 00 00 09 91 8b 0b 7a 41 67 61 73 70 00 00 0e 38 00 00 00 08 00 00 00 08 00 00 00 10 67 6c 79 66 00 00 0e 40 00 00 40 76 00 00 70 58 80 78 59 fa 68 65 61 64 00 00 4e b8 00 00 00 Data Ascii: wOFFW4FFTMcTNGDEF GPOS-rBGSUBbOS/2``lcmaplolcvt 2<+sfpgm<zAgasp8glyf@@vpXxYheadN
2022-05-27 05:41:16 UTC	551	IN	Data Raw: 77 b3 0f d9 37 8b 51 2e 8e 62 70 ec 92 d4 99 53 a7 35 be 7d e6 62 eb 05 65 e7 29 41 27 9a 0d 4e 67 2c fa 09 5d 43 01 5c 3e 89 7b ef 40 a6 20 a6 f6 c8 36 b2 c5 91 64 8f 48 9f c6 51 0d c5 ce 7b 35 ba 5f 7e 11 c6 b1 59 ec bc fb 9a c4 33 f6 5c 25 9b 03 83 af ca 01 5d 17 0f 16 f4 bb b9 ad 74 f0 b4 0f ce 09 8d 16 e5 aa 27 9c a6 6c cb 4a 1b 8d 46 b7 d1 ed f6 d8 7d dc 60 45 19 28 c1 09 6e bc 88 db 03 70 b6 e1 f1 87 97 af aa 47 56 6c 86 ae d0 e5 91 fb a0 bc 81 6d 62 cf 49 b9 e3 27 37 8e 69 9d db 7a 58 d9 f9 e1 89 85 87 8a 99 e3 51 9a c7 59 50 8f f6 c9 8d ba 30 c0 e3 fe 24 d4 85 c9 2a d5 dd 78 8c fb db 15 60 bb d7 ee ef a6 0b 04 0f 3b da 42 ea ee 10 e8 4e 31 fa e0 ae 8a c6 9d 14 f4 d7 bb 80 bb 0b c8 6e f6 29 fb 6a c7 13 ef 8d 9a 34 ad e7 cd cb 1f 78 60 04 68 5f dc Data Ascii: w7Q.bpS5}be)A'Ng,]C\>{@ 6dHQ{5_~Y3\%]t'lJF}`E(npGVlmbI'7izXQYP0$*x`;BN1n)j4x`h_
2022-05-27 05:41:16 UTC	583	IN	Data Raw: a4 b0 62 58 4e 69 ff b2 01 77 ac b9 75 ef df 0a f3 fe d9 33 b3 aa 24 bb 5f 71 f9 f8 fd 7c 9e d9 28 2f 3c 7f a7 f1 5c 07 ae 20 d0 4a e1 50 b4 29 7e 5d 5d e8 1a 91 9e 61 6f b3 59 f2 08 7c ed 00 ca 18 3e bf 15 65 bd 1e 9f b7 73 dd ca 93 a6 fa 91 45 84 2a fc db 4e ec 5e 87 4f b1 e7 80 cd a9 ca b8 ea 5c 99 e9 51 87 4d a9 5f c1 ce fe 91 7d c6 de 82 82 07 7f b5 1a 15 6c 4b c5 ba f3 f7 81 e7 92 b4 b5 65 e1 0b cf fe 7a b3 d4 ac ef 5d ae 61 82 42 87 e3 3c 8d dc dd 2f e1 db 35 12 f3 e3 3c 25 c4 e0 11 7f 90 43 85 45 d2 45 28 66 b1 6c 2b 8b 83 62 70 b8 f3 54 73 48 4f 2e b5 ac 19 f6 5e 56 dd 67 3a 4c 6d 37 c2 4c e5 73 4f 88 55 78 ea a3 84 e7 43 da f5 65 82 db 96 a0 5b 3e 29 93 06 30 16 e6 be 94 83 07 7f 45 0e 8f 03 11 89 37 ea 60 f6 eb 03 e6 02 59 ed 19 b3 1f 75 e9 43 Data Ascii: bXNiwu3$_q|(/<\ JP)~]]aoY|>esE*N^O\QM_}lKez]aB</5<%CEE(fl+bpTsHO.^Vg:Lm7LsOUxCe[>)0E7`YuC
2022-05-27 05:41:16 UTC	591	IN	Data Raw: 30 83 d1 20 1b 8c 72 e3 15 fd 19 06 83 b5 b4 53 93 86 a9 ad 38 a7 38 fa b9 8e dd 1a 1d 9f 33 5d d9 b2 91 e8 f3 01 f8 ba f9 ba 65 67 f1 a3 11 48 84 44 de ba 61 b7 a4 e5 5c 93 86 3b a7 09 1a b2 fd ff bf d1 90 15 b8 26 0d e9 9d 68 38 f0 c3 65 f2 db 50 5c cf ae 99 92 c1 d8 99 88 42 7e 29 9e 51 c6 09 5d 49 85 d1 78 05 15 e6 36 2a 7a 77 78 b0 23 19 1d 1f 34 5f 49 46 b2 20 23 cf 97 97 db 79 31 62 d2 c2 f6 4d a7 c5 da 89 96 b7 4c 84 fc 31 64 8a 50 11 e9 f2 e9 df 79 ee b1 60 30 98 30 d0 35 99 ac a5 31 60 34 9a ab 89 d9 6c e9 4c 8d b5 8d 9a 92 ce 34 fc 24 00 eb 95 54 79 fc 48 d5 75 85 bd 82 79 3d ba 75 cd 0a f8 fa f8 fb 74 a0 2d ae 23 6d 72 27 da 9a 54 42 7e 75 25 6d c1 ce b4 f1 db 0a 0d d5 e8 b2 5d 29 64 96 36 82 8a 3a 13 74 f5 a7 2c 57 11 31 80 de d7 f5 ca ef de Data Ascii: 0 rS883]egHDa\;&h8eP\B~)Q]lx6*zwx#4_IF #y1bML1dPy`0051`4lL4$TyHuy=ut-#mr'TB~u%m])d6:t,W1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49864	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:16 UTC	525	OUT	GET /cPanel_magic_revision_1463518546/unprotected/cpanel/images/notice-info.png HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://webmail.serendahsteel.com/cPanel_magic_revision_1630269605/unprotected/cpanel/style_v2_optimized.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: webmailsession=%3arZynwdYmgajDMd6a%2c10841453a97a6117ead87650119bd7a3; session_locale=en; roundcube_cookies=enabled

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:16 UTC	552	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:16 GMT Server: Apache Content-Type: image/png Last-Modified: Tue, 17 May 2016 20:55:46 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:16 GMT Content-Length: 976 Connection: close
2022-05-27 05:41:16 UTC	552	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 1c 00 00 00 1c 08 06 00 00 00 72 0d df 94 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 88 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 0b 11 00 00 0b 11 01 7f 64 5f 91 00 00 00 15 74 45 58 74 43 72 65 61 74 69 6f 6e 20 54 69 6d 65 00 37 2f 32 35 2f 31 32 66 c3 ef fb 00 00 00 1c 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 46 69 72 65 77 6f 72 6b 73 20 43 53 34 06 b2 d3 a0 00 00 03 0c 49 44 41 54 48 4b bd 96 5d 68 52 61 18 c7 07 96 41 c8 ae 2a a4 75 23 84 78 b9 24 a8 0b 57 d1 6d 84 bb 19 86 63 c8 82 a2 a2 4c 89 09 05 42 37 16 b3 0f a4 e8 43 49 57 ae 05 82 7a ad 77 bb f1 62 32 44 50 50 74 83 e1 c6 14 05 61 03 a7 5e d9 Data Ascii: PNGIHDRrsBIT|dsRGBgAMAapHYsd_tEXtCreation Time7/25/12ftEXtSoftwareAdobe Fireworks CS4IDA THK]hRaA*u#x$WmcLB7ClWzwb2DPPta^

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49825	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:06 UTC	42	OUT	GET /cPanel_magic_revision_1386192030/unprotected/cpanel/fonts/open_sans/open_sans.min.css HTTP/1.1 Host: webmail.unitedyacht.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: style Referer: https://arthurperush.com/css/cPanel.SharePoint_documentOnline/login.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 05:41:07 UTC	51	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:06 GMT Server: Apache/2.4.53 (cPanel) OpenSSL/1.1.1o mod_bwlimited/1.4 Content-Type: text/css Last-Modified: Tue, 23 Mar 2021 16:37:21 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:06 GMT Content-Length: 6358 Vary: Accept-Encoding,User-Agent Connection: close
2022-05-27 05:41:07 UTC	52	IN	Data Raw: 40 66 6f 6e 74 2d 66 61 63 65 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 27 4f 70 65 6e 20 53 61 6e 73 27 3b 73 72 63 3a 75 72 6c 28 2f 63 50 61 6e 65 6c 5f 6d 61 67 69 63 5f 72 65 76 69 73 69 6f 6e 5f 31 36 31 36 35 31 37 34 34 31 2f 75 6e 70 72 6f 74 65 63 74 65 64 2f 63 70 61 6e 65 6c 2f 66 6f 6e 74 73 2f 6f 70 65 6e 5f 73 61 6e 73 2f 4f 70 65 6e 53 61 6e 73 2d 42 6f 6c 64 2d 77 65 62 66 6f 6e 74 2e 65 6f 74 29 3b 73 72 63 3a 75 72 6c 28 2f 63 50 61 6e 65 6c 5f 6d 61 67 69 63 5f 72 65 76 69 73 69 6f 6e 5f 31 36 31 36 35 31 37 34 34 31 2f 75 6e 70 72 6f 74 65 63 74 65 64 2f 63 70 61 6e 65 6c 2f 66 6f 6e 74 73 2f 6f 70 65 6e 5f 73 61 6e 73 2f 4f 70 65 6e 53 61 6e 73 2d 42 6f 6c 64 2d 77 65 62 66 6f 6e 74 2e 65 6f 74 3f 23 69 65 66 69 78 29 20 66 6f 72 6d 61 Data Ascii: @font-face{font-family:'Open Sans';src:url(/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Bold-webfont.eot);src:url(/cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Bold-webfont.eot?#iefix) forma

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49865	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:16 UTC	525	OUT	GET /cPanel_magic_revision_1463518546/unprotected/cpanel/images/notice-error.png HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://webmail.serendahsteel.com/cPanel_magic_revision_1630269605/unprotected/cpanel/style_v2_optimized.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: webmailsession=%3arZynwdYmgajDMd6a%2c10841453a97a6117ead87650119bd7a3; session_locale=en; roundcube_cookies=enabled
2022-05-27 05:41:16 UTC	552	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:16 GMT Server: Apache Content-Type: image/png Last-Modified: Tue, 17 May 2016 20:55:46 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:16 GMT Content-Length: 1026 Connection: close
2022-05-27 05:41:16 UTC	553	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 1c 00 00 00 1c 08 06 00 00 00 72 0d df 94 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 88 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 0b 11 00 00 0b 11 01 7f 64 5f 91 00 00 00 15 74 45 58 74 43 72 65 61 74 69 6f 6e 20 54 69 6d 65 00 37 2f 32 35 2f 31 32 66 c3 ef fb 00 00 00 1c 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 46 69 72 65 77 6f 72 6b 73 20 43 53 34 06 b2 d3 a0 00 00 03 3e 49 44 41 54 48 4b bd 96 df 4b 93 51 18 c7 d5 d9 ac 30 2f 42 70 ec aa 51 98 c6 22 a2 ee 9a 26 74 31 ba 88 ad 0b 2b bc f1 2e cd 22 1c e1 a2 20 88 92 ae fa 9d 34 93 b2 b6 b5 86 17 db 95 37 13 ff 02 f1 42 10 77 23 a2 43 19 b2 8b c9 84 31 ef Data Ascii: PNGIHDRrsBIT|dsRGBgAMAapHYsd_tEXtCreation Time7/25/12ftEXtSoftwareAdobe Fireworks CS4>ID ATHKKQ0/BpQ"&t1+." 47Bw#C1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49866	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:16 UTC	526	OUT	GET /cPanel_magic_revision_1463518546/unprotected/cpanel/images/icon-username.png HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://webmail.serendahsteel.com/cPanel_magic_revision_1630269605/unprotected/cpanel/style_v2_optimized.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: webmailsession=%3arZynwdYmgajDMd6a%2c10841453a97a6117ead87650119bd7a3; session_locale=en; roundcube_cookies=enabled
2022-05-27 05:41:16 UTC	554	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:16 GMT Server: Apache Content-Type: image/png Last-Modified: Tue, 17 May 2016 20:55:46 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:16 GMT Content-Length: 320 Connection: close
2022-05-27 05:41:16 UTC	554	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 14 00 00 00 14 08 06 00 00 00 8d 89 1d 0d 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 88 00 00 00 09 70 48 59 73 00 00 0b 12 00 00 0b 12 01 d2 dd 7e fc 00 00 00 1c 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 46 69 72 65 77 6f 72 6b 73 20 43 53 34 06 b2 d3 a0 00 00 00 15 74 45 58 74 43 72 65 61 74 69 6f 6e 20 54 69 6d 65 00 36 2f 32 39 2f 31 31 13 6b 0a 4d 00 00 00 99 49 44 41 54 38 cb 63 f8 ff ff 3f 03 35 31 82 81 06 d8 6c 3c d9 81 d8 0a 88 e3 80 b8 18 4a cb 82 c4 41 f2 e4 18 18 0e 35 08 1d 87 93 6b 60 31 2e 3c 0c 0d 04 6a 32 c6 67 20 48 9e 54 03 ad 08 18 68 45 aa 81 2a 78 0c cb 01 c9 93 13 86 b8 5c a9 4d 6e a4 b0 23 25 6a 18 8e 83 c9 93 6c 20 0e 57 5a 51 6a a0 3f 9a 81 fe 24 1b 08 8d Data Ascii: PNGIHDRsBIT|dpHYs~tEXtSoftwareAdobe Fireworks CS4tEXtCreation Time6/29/11kMIDAT8c?51l<JA5k`1.<j2g HThE*x\Mn#%jl WZQj?$

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49872	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:17 UTC	597	OUT	GET /cPanel_magic_revision_1463518546/unprotected/cpanel/images/icon-password.png HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://webmail.serendahsteel.com/cPanel_magic_revision_1630269605/unprotected/cpanel/style_v2_optimized.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: webmailsession=%3arZynwdYmgajDMd6a%2c10841453a97a6117ead87650119bd7a3; session_locale=en; roundcube_cookies=enabled
2022-05-27 05:41:17 UTC	599	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:17 GMT Server: Apache Content-Type: image/png Last-Modified: Tue, 17 May 2016 20:55:46 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:17 GMT Content-Length: 450 Connection: close
2022-05-27 05:41:17 UTC	599	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 14 00 00 00 14 08 06 00 00 00 8d 89 1d 0d 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 88 00 00 00 09 70 48 59 73 00 00 0b 12 00 00 0b 12 01 d2 dd 7e fc 00 00 00 1c 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 46 69 72 65 77 6f 72 6b 73 20 43 53 34 06 b2 d3 a0 00 00 00 15 74 45 58 74 43 72 65 61 74 69 6f 6e 20 54 69 6d 65 00 36 2f 32 39 2f 31 31 13 6b 0a 4d 00 00 01 1b 49 44 41 54 38 cb 63 f8 ff ff 3f 03 35 31 2a 07 09 b0 d9 78 b2 03 b1 15 10 e7 00 71 31 14 a7 82 c4 40 f2 24 19 08 32 8c dd d6 2b 0e 64 88 80 4b 60 92 7e 4c ba 2b 08 0b bb 07 c7 40 0d f6 27 c9 40 0e 5b 2f 47 90 46 97 dc 32 2b a0 b8 30 10 f3 40 b1 20 48 0c 6a a8 15 29 2e 2c 96 f6 89 08 07 8a 71 32 a0 01 90 98 42 60 4c 20 a7 Data Ascii: PNGIHDRsBIT|dpHYs~tEXtSoftwareAdobe Fireworks CS4tEXtCreation Time6/29/11kMIDAT8c?51*xq1 @$2+dK`~L+@'@[/GF2+0@ Hj).,q2B`L

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49871	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:17 UTC	598	OUT	GET /cPanel_magic_revision_1463518546/unprotected/cpanel/images/notice-success.png HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://webmail.serendahsteel.com/cPanel_magic_revision_1630269605/unprotected/cpanel/style_v2_optimized.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: webmailsession=%3arZynwdYmgajDMd6a%2c10841453a97a6117ead87650119bd7a3; session_locale=en; roundcube_cookies=enabled
2022-05-27 05:41:17 UTC	600	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:17 GMT Server: Apache Content-Type: image/png Last-Modified: Tue, 17 May 2016 20:55:46 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:17 GMT Content-Length: 962 Connection: close
2022-05-27 05:41:17 UTC	600	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 1c 00 00 00 1c 08 06 00 00 00 72 0d df 94 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 88 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 0b 11 00 00 0b 11 01 7f 64 5f 91 00 00 00 15 74 45 58 74 43 72 65 61 74 69 6f 6e 20 54 69 6d 65 00 37 2f 32 35 2f 31 32 66 c3 ef fb 00 00 00 1c 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 46 69 72 65 77 6f 72 6b 73 20 43 53 34 06 b2 d3 a0 00 00 02 fe 49 44 41 54 48 4b bd 96 4d 68 92 71 1c c7 07 92 45 c9 88 f0 f0 a4 87 18 98 0c 56 10 96 b0 cb 56 5d 8a 88 70 11 42 08 b1 43 14 bd c1 18 91 a7 1d ba d4 c5 82 a6 50 6c 94 99 b5 c0 83 82 27 11 0f 3b 0e 64 87 9d 86 30 76 da 10 11 15 1c 82 2f Data Ascii: PNGIHDRrsBIT|dsRGBgAMAapHYsd_tEXtCreation Time7/25/12ftEXtSoftwareAdobe Fireworks CS4IDA THKMhqEVV]pBCPl';d0v/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49873	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:17 UTC	598	OUT	GET /cPanel_magic_revision_1463518546/unprotected/cpanel/images/warning.png HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://webmail.serendahsteel.com/cPanel_magic_revision_1630269605/unprotected/cpanel/style_v2_optimized.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: webmailsession=%3arZynwdYmgajDMd6a%2c10841453a97a6117ead87650119bd7a3; session_locale=en; roundcube_cookies=enabled
2022-05-27 05:41:17 UTC	601	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:17 GMT Server: Apache Content-Type: image/png Last-Modified: Tue, 17 May 2016 20:55:46 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:17 GMT Content-Length: 1060 Connection: close
2022-05-27 05:41:17 UTC	601	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 1c 00 00 00 1c 08 06 00 00 00 72 0d df 94 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 88 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 0b 11 00 00 0b 11 01 7f 64 5f 91 00 00 00 15 74 45 58 74 43 72 65 61 74 69 6f 6e 20 54 69 6d 65 00 37 2f 32 35 2f 31 32 66 c3 ef fb 00 00 00 1c 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 46 69 72 65 77 6f 72 6b 73 20 43 53 34 06 b2 d3 a0 00 00 03 60 49 44 41 54 48 4b bd 96 4b 48 1b 51 14 86 9d a6 6a 9b 34 6d 63 9f c6 d2 a6 d6 3e 56 96 36 8b 2e ba 89 29 56 52 9b ee 63 da 55 41 11 23 d6 d8 2e 12 62 90 52 a8 c4 a4 92 d8 a6 b3 49 8a d1 64 e9 46 44 45 7c a1 82 41 d1 85 e2 0b 14 df a2 e2 Data Ascii: PNGIHDRrsBIT|dsRGBgAMAapHYsd_tEXtCreation Time7/25/12ftEXtSoftwareAdobe Fireworks CS4`ID ATHKKHQj4mc>V6.)VRcUA#.bRIdFDE|A

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49884	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:20 UTC	602	OUT	GET /?locale=ar HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: webmailsession=%3arZynwdYmgajDMd6a%2c10841453a97a6117ead87650119bd7a3; session_locale=en; roundcube_cookies=enabled; timezone=America/Los_Angeles

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:21 UTC	603	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:21 GMT Server: Apache Content-Type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 38811 Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: webmailsession=%3aL_5UxxdUFcs79CER%2cca816adc682c985b33878010947b95b9; HttpOnly; path=/; port=443; secure Set-Cookie: session_locale=ar; expires=Sat, 27-May-2023 05:41:21 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 0 0:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00 :00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=443; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: imp_key=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00 :00:01 GMT; path=/; port=443 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 27-May-2023 05:41:21 GMT; path=/; port=443; secure Connection: close
2022-05-27 05:41:21 UTC	605	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 61 72 22 20 64 69 72 3d 22 72 74 6c 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f Data Ascii: <!DOCTYPE html><html lang="ar" dir="rtl"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1"> <meta name="goo
2022-05-27 05:41:21 UTC	611	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 69 63 6f 6e 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 69 63 6f 6e 22 3e 3c 2f 73 70 61 6e 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 6d 65 73 73 61 67 65 22 3e 54 68 65 20 73 79 73 74 65 6d 20 68 61 73 20 64 65 74 65 63 74 65 64 20 74 68 61 74 20 79 6f 75 20 61 72 65 20 75 73 69 6e 67 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 63 50 61 6e 65 6c 20 26 61 6d 70 3b 20 57 48 4d 20 6e 6f 20 6c 6f 6e 67 65 72 20 73 75 70 70 6f 72 74 73 20 49 6e 74 65 72 6e 65 74 20 45 78 Data Ascii: The system has detected that you are using Internet Explorer 11. cPanel & WHM no l onger supports Internet Ex
2022-05-27 05:41:21 UTC	613	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 65 73 5f 65 73 22 3e 65 73 70 61 c3 b1 6f 6c 20 64 65 20 45 73 70 61 c3 b1 61 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 22 3e 73 75 6f 6d 69 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 Data Ascii: espaol de Espaa suomi
2022-05-27 05:41:21 UTC	621	IN	Data Raw: 73 69 6c 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 72 6f 27 3e 72 6f 6d c3 a2 6e c4 83 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 72 75 27 3e d1 80 d1 83 d1 81 d1 81 d0 ba d0 b8 d0 b9 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 73 6c 27 3e 73 6c 6f 76 65 6e c5 a1 c4 8d 69 6e 61 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 73 76 27 3e 73 76 65 6e 73 6b 61 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 74 68 27 3e e0 b9 84 e0 b8 97 e0 b8 a2 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 74 72 27 3e 54 c3 bc 72 6b c3 a7 65 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 75 Data Ascii: sil</option><option value='ro'>romn</option><option value='ru'></option><option value='sl'>slovenina</option ><option value='sv'>svenska</option><option value='th'></option><option value='tr'>Trke</option><option value='u
2022-05-27 05:41:21 UTC	627	IN	Data Raw: 69 67 61 74 6f 72 2e 75 73 65 72 41 67 65 6e 74 2e 69 6e 64 65 78 4f 66 28 22 54 72 69 64 65 6e 74 22 29 21 3d 3d 2d 31 29 7b 76 61 72 20 69 65 42 61 6e 6e 65 72 44 69 76 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 49 45 2d 77 61 72 6e 69 6e 67 22 29 3b 69 66 28 69 65 42 61 6e 6e 65 72 44 69 76 29 7b 69 65 42 61 6e 6e 65 72 44 69 76 2e 63 6c 61 73 73 4c 69 73 74 2e 72 65 6d 6f 76 65 28 22 49 45 2d 77 61 72 6e 69 6e 67 2d 68 69 64 65 22 29 7d 7d 7d 73 68 6f 77 49 45 42 61 6e 6e 65 72 28 29 3b 66 75 6e 63 74 69 6f 6e 20 66 61 64 65 5f 69 6e 28 65 6c 2c 64 75 72 61 74 69 6f 6e 2c 5f 66 61 64 65 5f 6f 75 74 5f 69 6e 73 74 65 61 64 29 7b 65 6c 3d 64 69 76 5f 63 61 63 68 65 5b 65 6c 5d 7c 7c 44 4f 4d 2e 67 65 74 28 65 6c 29 7c Data Ascii: igator.userAgent.indexOf("Trident")!==-1){var ieBannerDiv=document.getElementById("IE-warning");if (ieBannerDiv){ieBannerDiv.classList.remove("IE-warning-hide")}}}showIEBanner();function fade_in(el,duration,_f ade_out_instead){el=div_cache[el]||DOM.get(el)|

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:21 UTC	629	IN	Data Raw: 75 65 29 3b 61 6a 61 78 2e 73 65 6e 64 28 6e 75 6c 6c 29 7d 74 68 69 73 2e 41 4a 41 58 3d 61 6a 61 78 3b 74 68 69 73 2e 75 70 64 61 74 69 6e 67 3d 74 72 75 65 7d 63 61 74 63 68 28 65 29 7b 6c 6f 67 69 6e 5f 66 6f 72 6d 2e 73 75 62 6d 69 74 28 29 7d 72 65 74 75 72 6e 20 74 72 75 65 7d 3b 76 61 72 20 5f 74 65 78 74 5f 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 43 6f 6e 74 65 6e 74 22 69 6e 20 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 3f 22 74 65 78 74 43 6f 6e 74 65 6e 74 22 3a 22 69 6e 6e 65 72 54 65 78 74 22 3b 66 75 6e 63 74 69 6f 6e 20 5f 70 72 6f 63 65 73 73 5f 70 61 72 73 65 64 5f 6c 6f 67 69 6e 5f 73 75 63 63 65 73 73 28 72 65 73 75 6c 74 29 7b 76 61 72 20 66 69 6e 61 6c 5f 75 72 69 3b 76 61 72 20 6c 6f 67 69 6e 5f 75 72 6c 5f 72 65 67 65 78 3d 2f 5e 5c 2f Data Ascii: ue);ajax.send(null)}this.AJAX=ajax;this.updating=true}catch(e){login_form.submit()}return true};var _text_content="textContent"in document.body?"textContent":"innerText";function _process_parsed_login_success(result){var final_uri;var login_url_regex=/^\/
2022-05-27 05:41:21 UTC	637	IN	Data Raw: 75 6c 22 3a 6e 65 77 20 44 61 74 65 28 32 30 31 31 2c 32 2c 32 38 2c 35 2c 30 2c 30 2c 30 29 2c 22 41 73 69 61 2f 44 61 6d 61 73 63 75 73 22 3a 6e 65 77 20 44 61 74 65 28 32 30 31 31 2c 33 2c 31 2c 32 2c 30 2c 30 2c 30 29 2c 22 41 73 69 61 2f 4a 65 72 75 73 61 6c 65 6d 22 3a 6e 65 77 20 44 61 74 65 28 32 30 31 31 2c 33 2c 31 2c 36 2c 30 2c 30 2c 30 29 2c 22 41 73 69 61 2f 47 61 7a 61 22 3a 6e 65 77 20 44 61 74 65 28 32 30 30 39 2c 32 2c 32 38 2c 30 2c 33 30 2c 30 2c 30 29 2c 22 41 66 72 69 63 61 2f 43 61 69 72 6f 22 3a 6e 65 77 20 44 61 74 65 28 32 30 30 39 2c 33 2c 32 35 2c 30 2c 33 30 2c 30 2c 30 29 2c 22 50 61 63 69 66 69 63 2f 41 75 63 6b 6c 61 6e 64 22 3a 6e 65 77 20 44 61 74 65 28 32 30 31 31 2c 38 2c 32 36 2c 37 2c 30 2c 30 2c 30 29 2c 22 50 61 63 Data Ascii: ul":new Date(2011,2,28,5,0,0,0),"Asia/Damascus":new Date(2011,3,1,2,0,0,0),"Asia/Jerusalem":new Date(2011,3,1,6,0,0,0),"Asia/Gaza":new Date(2009,2,28,0,30,0,0),"Africa/Cairo":new Date(2009,3,25,0,30,0,0),"Pacific/Auckland":new Date(2011,8,26,7,0,0,0),"Pac
2022-05-27 05:41:21 UTC	642	IN	Data Raw: 68 2e 63 61 6c 6c 28 64 65 74 65 63 74 65 64 5f 6e 6f 64 65 73 2c 28 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 6e 2e 74 65 78 74 43 6f 6e 74 65 6e 74 3d 64 65 74 65 63 74 65 64 5f 74 7a 7d 29 29 3b 76 61 72 20 73 68 6f 77 5f 6e 6f 64 65 73 3d 64 6f 63 75 6d 65 6e 74 2e 71 75 65 72 79 53 65 6c 65 63 74 6f 72 41 6c 6c 28 22 2e 22 2b 43 4f 4f 4b 49 45 5f 54 49 4d 45 5a 4f 4e 45 5f 4d 49 53 4d 41 54 43 48 5f 43 4c 41 53 53 29 3b 5b 5d 2e 66 6f 72 45 61 63 68 2e 63 61 6c 6c 28 73 68 6f 77 5f 6e 6f 64 65 73 2c 28 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 6e 2e 63 6c 61 73 73 4e 61 6d 65 2b 3d 22 20 22 2b 53 48 4f 57 4e 5f 43 4c 41 53 53 7d 29 29 7d 7d 77 69 6e 64 6f 77 2e 43 50 54 69 6d 65 7a 6f 6e 65 3d 7b 73 68 6f 77 5f 63 6f 6f 6b 69 65 5f 74 69 6d 65 7a 6f 6e 65 5f 6d Data Ascii: h.call(detected_nodes,(function(n){n.textContent=detected_tz}));var show_nodes=document.querySelectorAll("."+COOKIE_TIMEZONE_MISMATCH_CLASS);[].forEach.call(show_nodes,(function(n){n.className+=" "+SHOWN_CLASS}))}}window.CPTimezone={show_cookie_timezone_m

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49885	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:24 UTC	643	OUT	GET /?locale=bg HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: roundcube_cookies=enabled; timezone=America/Los_Angeles; webmailsession=%3aL_5UxxdUFcs79CER%2cca816adc682c985b33878010947b95b9; session_locale=ar

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:25 UTC	644	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:25 GMT Server: Apache Content-Type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 37802 Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: webmailsession=%3aXM1wd6prSVQkUfND%2ca2ab7509298ff536dc5d34c974c32524; HttpOnly; path=/; port=443; secure Set-Cookie: session_locale=bg; expires=Sat, 27-May-2023 05:41:25 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 0 0:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00 :00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=443; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: imp_key=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00 :00:01 GMT; path=/; port=443 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 27-May-2023 05:41:25 GMT; path=/; port=443; secure Connection: close
2022-05-27 05:41:25 UTC	646	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 62 67 22 20 64 69 72 3d 22 6c 74 72 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f Data Ascii: <!DOCTYPE html><html lang="bg" dir="ltr"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1"> <meta name="goo
2022-05-27 05:41:25 UTC	652	IN	Data Raw: 67 65 22 3e 54 68 65 20 73 79 73 74 65 6d 20 68 61 73 20 64 65 74 65 63 74 65 64 20 74 68 61 74 20 79 6f 75 20 61 72 65 20 75 73 69 6e 67 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 63 50 61 6e 65 6c 20 26 61 6d 70 3b 20 57 48 4d 20 6e 6f 20 6c 6f 6e 67 65 72 20 73 75 70 70 6f 72 74 73 20 49 6e 74 65 72 6e 65 74 2 0 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 72 65 61 64 2 0 74 68 65 20 3c 61 20 74 69 74 6c 65 3d 22 63 50 61 6e 65 6c 20 42 6c 6f 67 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6f 2e 63 70 61 6e 65 6c 2e 6e 65 74 2f 69 65 31 31 64 65 70 72 65 63 61 74 69 6f 6e 22 3e 63 50 61 6e 65 6c 20 42 6c 6f 67 3c 2f Data Ascii: ge">The system has detected that you are using Internet Explorer 11. cPanel & WHM no longer supports Internet Explorer 11. For more information, read the <a title="cPanel Blog" target="_blank" href="https://go.cpanel.net/ie1 1deprecation">cPanel Blog</
2022-05-27 05:41:25 UTC	654	IN	Data Raw: 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 22 3e 73 75 6f 6d 69 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 6c 22 3e 46 69 6c 69 70 69 6e 6f 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 6 5 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d Data Ascii: ll">suomi</div> <div class="locale-cell">Filipino</div> <div class="locale-cell"><a href="?locale=
2022-05-27 05:41:25 UTC	662	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 62 75 74 74 6f 6e 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 31 30 70 78 22 20 74 79 70 65 3d 22 73 75 62 6d 69 74 22 3e 43 68 61 6e 67 65 3c 2f 62 75 74 74 6f 6e 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 66 6f 72 6d 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 23 6d 6 f 62 69 6c 65 6c 6f 63 61 6c 65 6d 65 6e 75 2c 20 23 6c 6f 63 61 6c 65 73 5f 6c 69 73 74 20 7b 64 69 73 70 6c 61 79 3a 6 e 6f 6e 65 7d 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 6e 6f 73 63 72 69 70 74 3 e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 75 6c 20 Data Ascii: <button style="margin-left: 10px" type="submit">Change</button> </form> <style type="text/css">#mobilelocalemenu, #locales_list {display:none}</style> </noscript> <ul
2022-05-27 05:41:25 UTC	667	IN	Data Raw: 61 74 69 6f 6e 5f 6d 73 2b 73 74 61 72 74 2e 67 65 74 54 69 6d 65 28 29 7d 65 6c 73 65 7b 73 74 79 6c 65 5f 6f 62 6a 2e 76 69 73 69 62 69 6c 69 74 79 3d 22 76 69 73 69 62 6c 65 22 7d 76 61 72 20 66 61 64 65 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 6f 70 61 63 69 74 79 3b 69 66 28 5f 66 61 64 65 5f 6f 75 74 5f 69 6e 73 74 65 61 64 29 7b 6f 70 61 63 69 74 79 3d 73 74 61 72 74 5f 6f 70 61 63 69 74 79 2a 28 65 6e 64 2d 6e 65 77 20 44 61 74 65 29 2f 64 75 72 61 74 69 6f 6e 5f 6d 73 3b 69 66 28 6f 70 61 63 69 74 79 3c 3d 30 29 7b 6f 70 61 63 69 74 79 3d 30 3b 63 6c 65 61 72 49 6e 74 65 72 76 61 6c 28 69 6e 74 65 72 76 61 6c 29 3b 73 74 79 6c 65 5f 6f 62 6a 2e 76 69 73 69 62 69 6c 69 74 79 3d 22 68 69 64 64 65 6e 22 7d 7d 65 6c 73 65 7b 6f 70 61 63 69 Data Ascii: ation_ms+start.getTime()}else{style_obj.visibility="visible"}var fader=function(){var opacity;if(_fade_out_i nstead){opacity=start_opacity*(end-new Date)/duration_ms;if(opacity<=0){opacity=0;clearInterval(interval);style_obj.visi bility="hidden"}}else{opaci

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:25 UTC	670	IN	Data Raw: 6f 74 69 63 65 73 22 29 3b 66 6f 72 28 76 61 72 20 6e 3d 30 3b 6e 3c 72 65 73 75 6c 74 2e 6e 6f 74 69 63 65 73 2e 6c 65 6e 67 74 68 3b 6e 2b 2b 29 7b 76 61 72 20 6e 65 77 5f 70 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 70 22 29 3b 6e 65 77 5f 70 2e 74 65 78 74 43 6f 6e 74 65 6e 74 3d 72 65 73 75 6c 74 2e 6e 6f 74 69 63 65 73 5b 6e 5d 2e 63 6f 6e 74 65 6e 74 3b 63 6f 6e 74 61 69 6e 65 72 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 6e 65 77 5f 70 29 7d 63 6c 69 63 6b 5f 66 6f 72 6d 2e 6f 6e 73 75 62 6d 69 74 3d 72 65 64 69 72 65 63 74 6f 72 3b 66 61 64 65 5f 6f 75 74 28 6c 6f 67 69 6e 5f 66 6f 72 6d 29 3b 66 61 64 65 5f 69 6e 28 63 6c 69 63 6b 5f 66 6f 72 6d 29 7d 65 6c 73 65 7b 73 68 6f 77 5f 73 74 61 74 75 73 28 4d 45 53 53 41 Data Ascii: otices");for(var n=0;n<result.notices.length;n++){var new_p=document.createElement("p");new_p.text Content=result.notices[n].content;container.appendChild(new_p)}click_form.onsubmit=redirector;fade_out(login_f orm);fade_in(click_form)}else{show_status(MESSA
2022-05-27 05:41:25 UTC	678	IN	Data Raw: 63 61 2f 4d 6f 6e 74 65 76 69 64 65 6f 22 3a 5b 22 41 6d 65 72 69 63 61 2f 4d 6f 6e 74 65 76 69 64 65 6f 22 2c 22 41 6d 65 72 69 63 61 2f 53 61 6f 5f 50 61 75 6c 6f 22 5d 2c 22 41 73 69 61 2f 42 65 69 72 75 74 22 3a 5b 22 41 73 69 61 2f 42 65 69 72 75 74 22 2c 22 45 75 72 6f 70 65 2f 48 65 6c 73 69 6e 6b 69 22 2c 22 45 75 72 6f 70 65 2f 49 73 74 61 6e 62 75 6c 22 2c 22 41 73 69 61 2f 44 61 6d 61 73 63 75 73 22 2c 22 41 73 69 61 2f 4a 65 72 75 73 61 6c 65 6d 22 2c 22 41 73 69 61 2f 47 61 7a 61 22 5d 2c 22 50 61 63 69 66 69 63 2f 41 75 63 6b 6c 61 6e 64 22 3a 5b 22 50 61 63 69 66 69 63 2f 41 75 63 6b 6c 61 6e 64 22 2c 22 50 61 63 69 66 69 63 2f 46 69 6a 69 22 5d 2c 22 41 6d 65 72 69 63 61 2f 4c 6f 73 5f 41 6e 67 65 6c 65 73 22 3a 5b 22 41 6d 65 72 69 63 61 Data Ascii: ca/Montevideo":["America/Montevideo","America/Sao_Paulo"],"Asia/Beirut":["Asia/Beirut","Europe/Helsinki","Eu rope/Istanbul","Asia/Damascus","Asia/Jerusalem","Asia/Gaza"],"Pacific/Auckland":["Pacific/Auckland","Pacific/Fiji"],"Ame rica/Los_Angeles":["America

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49902	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:28 UTC	682	OUT	GET /?locale=cs HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183. 121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig ned-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: roundcube_cookies=enabled; timezone=America/Los_Angeles; webmailsession=%3aXM1wd6prSVQkUfND% 2ca2ab7509298ff536dc5d34c974c32524; session_locale=bg
2022-05-27 05:41:29 UTC	683	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:29 GMT Server: Apache Content-Type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 38244 Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: webmailsession=%3a3Be1T1zsuDYpXraK%2c161f27175e3ad11afbd2948b84e08c4f; HttpOnly; path=/; port=443; secure Set-Cookie: session_locale=cs; expires=Sat, 27-May-2023 05:41:28 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 0 0:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00 :00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=443; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: imp_key=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00 :00:01 GMT; path=/; port=443 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 27-May-2023 05:41:28 GMT; path=/; port=443; secure Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:29 UTC	685	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 63 73 22 20 64 69 72 3d 22 6c 74 72 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f Data Ascii: <!DOCTYPE html><html lang="cs" dir="ltr"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1"> <meta name="goo
2022-05-27 05:41:29 UTC	691	IN	Data Raw: 6c 61 73 73 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 69 63 6f 6e 22 3e 3c 2f 73 70 61 6e 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 6d 65 73 73 61 67 65 22 3e 54 68 65 20 73 79 73 74 65 6d 20 68 61 73 20 64 65 74 65 63 74 65 64 20 74 68 61 74 20 79 6f 75 20 61 72 65 20 75 73 69 6e 67 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 63 50 61 6e 65 6c 20 26 61 6d 70 3b 20 57 48 4d 20 6e 6f 20 6c 6f 6e 67 65 72 20 73 75 70 70 6f 72 74 73 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 72 65 61 64 20 74 68 65 20 3c 61 20 74 69 74 6c 65 3d 22 63 50 61 6e 65 Data Ascii: lass="IE-warning-icon"></div> <div id="IE-warning-message">The system has detected that you are using Internet Explorer 11. cPanel & WHM no longer supports Internet Explorer 11. For more information , read the <a title="cPane
2022-05-27 05:41:29 UTC	693	IN	Data Raw: 61 c3 b1 6f 6c 20 64 65 20 45 73 70 61 c3 b1 61 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 22 3e 73 75 6f 6d 69 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 6c 22 3e 46 69 6c 69 70 69 6e 6f 3c 2f 61 3e 3c Data Ascii: aol de Espaa</div> <div class="locale-cell">suomi</div> <div class="locale-cell">Filipino<
2022-05-27 05:41:29 UTC	701	IN	Data Raw: 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 75 6b 27 3e d1 83 d0 ba d1 80 d0 b0 d1 97 d0 bd d1 81 d1 8c d0 ba d0 b0 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 76 69 27 3e 54 69 e1 ba bf 6e 67 20 56 69 e1 bb 87 74 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 27 3e e4 b8 ad e6 96 87 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 5f 63 6e 27 3e e4 b8 ad e6 96 87 ef bc 88 e4 b8 ad e5 9b bd ef bc 89 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 5f 74 77 27 3e e4 b8 ad e6 96 87 ef bc 88 e5 8f b0 e6 b9 be ef bc 89 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 63 73 27 3e c4 8d 65 c5 a1 74 69 6e 61 3c 2f 6f Data Ascii: n><option value='uk'></option><option value='vi'>Ting Vit</option><option value='zh'></option><option value= 'zh_cn'></option><option value='zh_tw'></option><option value='cs'>etina</o
2022-05-27 05:41:29 UTC	707	IN	Data Raw: 6c 74 65 72 73 2e 69 74 65 6d 28 22 44 58 49 6d 61 67 65 54 72 61 6e 73 66 6f 72 6d 2e 4d 69 63 72 6f 73 6f 66 74 2e 41 6c 70 68 61 22 29 2e 6f 70 61 63 69 74 79 7d 63 61 74 63 68 28 65 29 7b 74 72 79 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 65 6c 2e 66 69 6c 74 65 72 73 28 22 61 6c 70 68 61 22 29 2e 6f 70 61 63 69 74 79 7d 63 61 74 63 68 28 65 72 72 6f 72 29 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 31 30 30 7d 7d 73 74 61 72 74 5f 6f 70 61 63 69 74 79 2f 3d 31 30 30 7d 69 66 28 21 73 74 61 72 74 5f 6f 70 61 63 69 74 79 29 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 30 7d 7d 65 6c 73 65 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 30 3b 73 65 74 5f 6f 70 61 63 69 74 79 28 65 6c 2c 30 29 7d 69 66 28 5f 66 61 64 65 5f 6f 75 74 5f 69 6e 73 74 65 61 Data Ascii: lters.item("DXImageTransform.Microsoft.Alpha").opacity}catch(e){try{start_opacity=el.filters("alpha").opacit y}catch(error){start_opacity=100}}start_opacity/=100}if(!start_opacity){start_opacity=0}}else{start_opacity=0;set_opacit y(el,0)}if(_fade_out_instea
2022-05-27 05:41:29 UTC	709	IN	Data Raw: 6c 65 6e 67 74 68 3b 66 2b 2b 29 7b 69 66 28 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 21 3d 3d 77 69 6e 64 6f 77 29 7b 76 61 72 20 68 72 65 66 3d 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 2e 72 65 70 6c 61 63 65 28 2f 5c 2f 63 70 73 65 73 73 5b 2e 5c 64 5d 2b 2f 2c 72 65 73 75 6c 74 2e 73 65 63 75 72 69 74 79 5f 74 6f 6b 65 6e 29 3b 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 68 72 65 66 7d 7d 7d 6c 6f 63 61 74 69 6f 6e 5f 6f 62 6a 5f 74 6f 5f 72 65 64 69 72 65 63 74 3d 6c 6f 63 61 74 69 6f 6e 7d 76 61 72 20 72 65 64 69 72 65 63 74 6f 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 6c 6f 63 61 74 69 6f 6e 5f 6f 62 6a 5f 74 6f 5f 72 65 64 69 72 65 63 74 2e 68 72 65 66 3d 66 69 6e 61 6c 5f Data Ascii: length;f++){if(top.frames[f]!==window){var href=top.frames[f].location.href.replace(/\/cpsess[.\d]+/,result. security_token);top.frames[f].location.href=href}}}location_obj_to_redirect=location}var redirector=function(){location_ obj_to_redirect.href=final_
2022-05-27 05:41:29 UTC	717	IN	Data Raw: 6b 75 74 73 6b 22 3a 74 2c 22 41 73 69 61 2f 59 61 6b 75 74 73 6b 22 3a 74 2c 22 41 73 69 61 2f 56 6c 61 64 69 76 6f 73 74 6f 6b 22 3a 74 2c 22 41 73 69 61 2f 4b 61 6d 63 68 61 74 6b 61 22 3a 74 2c 22 45 75 72 6f 70 65 2f 4d 69 6e 73 6b 22 3a 74 2c 22 41 75 73 74 72 61 6c 69 61 2f 50 65 72 74 68 22 3a 6e 65 77 20 44 61 74 65 28 32 30 30 38 2c 31 30 2c 31 2c 31 2c 30 2c 30 2c 30 29 7d 3b 72 65 74 75 72 6e 20 6e 5b 65 5d 7d 3b 72 65 74 75 72 6e 7b 64 65 74 65 72 6d 69 6e 65 3a 61 2c 64 61 74 65 5f 69 73 5f 64 73 74 3a 6f 2c 64 73 74 5f 73 74 61 72 74 5f 66 6f 72 3a 66 7d 7d 28 29 3b 74 2e 54 69 6d 65 5a 6f 6e 65 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 6e 3d 7b 22 41 6d 65 72 69 63 61 2f 44 65 6e 76 65 72 22 Data Ascii: kutsk":t,"Asia/Yakutsk":t,"Asia/Vladivostok":t,"Asia/Kamchatka":t,"Europe/Minsk":t,"Australia/Perth":new Dat e(2008,10,1,1,0,0,0)};return n[e]};return{determine:a,date_is_dst:o,dst_start_for:f}}();t.TimeZone=function(e){"use stri ct";var n={"America/Denver"
2022-05-27 05:41:29 UTC	722	IN	Data Raw: 5f 66 6f 72 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 70 78 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 70 79 72 69 67 68 74 22 3e 43 6f 70 79 72 69 67 68 74 c2 a9 c2 a0 32 30 32 32 20 63 50 61 6e 65 6c 2c 20 4c 2e 4c 2e 43 2e 0a 20 20 20 20 3c 62 72 20 2f 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6f 2e 63 70 61 6e 65 6c 2e 6e 65 74 2f 70 72 69 76 61 63 79 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 3e 50 72 69 76 61 63 79 20 50 6f 6c 69 63 79 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 0a 3c 2f 62 6f 64 79 3e 0a 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: _form { width: px; } }</style> <div class="copyright">Copyright2022 cPanel, L.L.C. Privacy Policy</div></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49933	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:30 UTC	722	OUT	GET /?locale=da HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: roundcube_cookies=enabled; timezone=America/Los_Angeles; webmailsession=%3a3Be1T1zsuDYpXraK%2c161f27175e3ad11afbd2948b84e08c4f; session_locale=cs
2022-05-27 05:41:31 UTC	723	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:31 GMT Server: Apache Content-Type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 38028 Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: webmailsession=%3arF9R3lM4ZLnbf_qE%2ce1f11a22c225092696e3c1e5bd9a25e4; HttpOnly; path=/; port=443; secure Set-Cookie: session_locale=da; expires=Sat, 27-May-2023 05:41:31 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=443; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: imp_key=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 27-May-2023 05:41:31 GMT; path=/; port=443; secure Connection: close
2022-05-27 05:41:31 UTC	725	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 64 61 22 20 64 69 72 3d 22 6c 74 72 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f Data Ascii: <!DOCTYPE html><html lang="da" dir="ltr"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1"> <meta name="goo
2022-05-27 05:41:31 UTC	731	IN	Data Raw: 61 67 65 22 3e 54 68 65 20 73 79 73 74 65 6d 20 68 61 73 20 64 65 74 65 63 74 65 64 20 74 68 61 74 20 79 6f 75 20 61 72 65 20 75 73 69 6e 67 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 63 50 61 6e 65 6c 20 26 61 6d 70 3b 20 57 48 4d 20 6e 6f 20 6c 6f 6e 67 65 72 20 73 75 70 70 6f 72 74 73 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 72 65 61 64 20 74 68 65 20 3c 61 20 74 69 74 6c 65 3d 22 63 50 61 6e 65 6c 20 42 6c 6f 67 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6f 2e 63 70 61 6e 65 6c 2e 6e 65 74 2f 69 65 31 31 64 65 70 72 65 63 61 74 69 6f 6e 22 3e 63 50 61 6e 65 6c 20 42 6c 6f 67 3c Data Ascii: age">The system has detected that you are using Internet Explorer 11. cPanel & WHM no longer supports Internet Explorer 11. For more information, read the <a title="cPanel Blog" target="_blank" href="https://go.cpanel.net/ie11deprecation">cPanel Blog<
2022-05-27 05:41:31 UTC	733	IN	Data Raw: 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 22 3e 73 75 6f 6d 69 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 6c 22 3e 46 69 6c 69 70 69 6e 6f 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 Data Ascii: s="locale-cell">suomi</div> <div class="locale-cell">Filipino</div> <div class="locale-cell"><a hr
2022-05-27 05:41:31 UTC	741	IN	Data Raw: 68 27 3e e4 b8 ad e6 96 87 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 5f 63 6e 27 3e e4 b8 ad e6 96 87 ef bc 88 e4 b8 ad e5 9b bd ef bc 89 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 5f 74 77 27 3e e4 b8 ad e6 96 87 ef bc 88 e5 8f b0 e6 b9 be ef bc 89 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 64 61 27 3e 64 61 6e 73 6b 3c 2f 6f 70 74 69 6f 6e 3e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 73 65 6c 65 63 74 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 62 75 74 74 6f 6e 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 31 30 70 78 22 20 74 79 70 65 3d 22 73 75 62 6d 69 74 22 3e Data Ascii: h'></option><option value='zh_cn'></option><option value='zh_tw'></option><option value='da'>dansk</option> </select> <button style="margin-left: 10px" type="submit">

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:31 UTC	747	IN	Data Raw: 30 3b 73 65 74 5f 6f 70 61 63 69 74 79 28 65 6c 2c 30 29 7d 69 66 28 5f 66 61 64 65 5f 6f 75 74 5f 69 6e 73 74 65 61 64 26 26 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3c 2e 30 31 29 7b 69 66 28 73 74 61 72 74 5f 6f 70 61 63 69 74 79 29 7b 73 65 74 5f 6f 70 61 63 69 74 79 28 65 6c 2c 30 29 7d 72 65 74 75 72 6e 7d 69 66 28 21 64 75 72 61 74 69 6f 6e 29 7b 64 75 72 61 74 69 6f 6e 3d 46 41 44 45 5f 44 55 52 41 54 49 4f 4e 7d 76 61 72 20 64 75 72 61 74 69 6f 6e 5f 6d 73 3d 64 75 72 61 74 69 6f 6e 2a 31 65 33 3b 76 61 72 20 73 74 61 72 74 3d 6e 65 77 20 44 61 74 65 3b 76 61 72 20 65 6e 64 3b 69 66 28 5f 66 61 64 65 5f 6f 75 74 5f 69 6e 73 74 65 61 64 29 7b 65 6e 64 3d 64 75 72 61 74 69 6f 6e 5f 6d 73 2b 73 74 61 72 74 2e 67 65 74 54 69 6d 65 28 29 7d 65 6c 73 65 Data Ascii: 0;set_opacity(el,0)}if(_fade_out_instead&&start_opacity<.01){if(start_opacity){set_opacity(el,0)}return}if(!duration){duration=FADE_DURATION}var duration_ms=duration*1e3;var start=new Date;var end;if(_fade_out_instead){end=duration_ms+start.getTime()}else
2022-05-27 05:41:31 UTC	749	IN	Data Raw: 28 29 7b 6c 6f 63 61 74 69 6f 6e 5f 6f 62 6a 5f 74 6f 5f 72 65 64 69 72 65 63 74 2e 68 72 65 66 3d 66 69 6e 61 6c 5f 75 72 69 2b 6c 6f 63 61 74 69 6f 6e 2e 68 61 73 68 7d 3b 69 66 28 72 65 73 75 6c 74 2e 6e 6f 74 69 63 65 73 26 26 72 65 73 75 6c 74 2e 6e 6f 74 69 63 65 73 2e 6c 65 6e 67 74 68 29 7b 73 68 6f 77 5f 73 74 61 74 75 73 28 4d 45 53 53 41 47 45 53 2e 72 65 61 64 5f 62 65 6c 6f 77 2c 22 77 61 72 6e 22 29 3b 76 61 72 20 63 6c 69 63 6b 5f 66 6f 72 6d 3d 44 4f 4d 2e 67 65 74 28 22 63 6c 69 63 6b 74 68 72 6f 75 67 68 5f 66 6f 72 6d 22 29 3b 76 61 72 20 63 6f 6e 74 61 69 6e 65 72 3d 63 6c 69 63 6b 5f 66 6f 72 6d 2e 71 75 65 72 79 53 65 6c 65 63 74 6f 72 28 22 2e 6e 6f 74 69 63 65 73 22 29 3b 66 6f 72 28 76 61 72 20 6e 3d 30 3b 6e 3c 72 65 73 75 6c 74 Data Ascii: (){location_obj_to_redirect.href=final_uri+location.hash};if(result.notices&&result.notices.length){show_status(MESSAGES.read_below,"warn");var click_form=DOM.get("clickthrough_form");var container=click_form.querySelector(".notices");for(var n=0;n<result
2022-05-27 05:41:31 UTC	757	IN	Data Raw: 65 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 6e 3d 7b 22 41 6d 65 72 69 63 61 2f 44 65 6e 76 65 72 22 3a 5b 22 41 6d 65 72 69 63 61 2f 44 65 6e 76 65 72 22 2c 22 41 6d 65 72 69 63 61 2f 4d 61 7a 61 74 6c 61 6e 22 5d 2c 22 41 6d 65 72 69 63 61 2f 43 68 69 63 61 67 6f 22 3a 5b 22 41 6d 65 72 69 63 61 2f 43 68 69 63 61 67 6f 22 2c 22 41 6d 65 72 69 63 61 2f 4d 65 78 69 63 6f 5f 43 69 74 79 22 5d 2c 22 41 6d 65 72 69 63 61 2f 53 61 6e 74 69 61 67 6f 22 3a 5b 22 41 6d 65 72 69 63 61 2f 53 61 6e 74 69 61 67 6f 22 2c 22 41 6d 65 72 69 63 61 2f 41 73 75 6e 63 69 6f 6e 22 2c 22 41 6d 65 72 69 63 61 2f 43 61 6d 70 6f 5f 47 72 61 6e 64 65 22 5d 2c 22 41 6d 65 72 69 63 61 2f 4d 6f 6e 74 65 76 69 64 65 6f 22 3a 5b 22 41 6d 65 72 69 63 61 2f 4d 6f 6e 74 Data Ascii: e){"use strict";var n={"America/Denver":["America/Denver","America/Mazatlan"],"America/Chicago":["America/Chicago","America/Mexico_City"],"America/Santiago":["America/Santiago","America/Asuncion","America/Campo_Grande"],"America/Montevideo":["America/Mont
2022-05-27 05:41:31 UTC	762	IN	Data Raw: 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: </html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49946	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:33 UTC	762	OUT	GET /?locale=de HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: roundcube_cookies=enabled; timezone=America/Los_Angeles; webmailsession=%3arF9R3lM4ZLnbf_qE%2ce1f11a22c225092696e3c1e5bd9a25e4; session_locale=da

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:33 UTC	763	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:33 GMT Server: Apache Content-Type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 38264 Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: webmailsession=%3aZEm_sI1rJvNEi7by%2c4ab193791d9e20fba6816ee2acc3df28; HttpOnly; path=/; port=443; secure Set-Cookie: session_locale=de; expires=Sat, 27-May-2023 05:41:33 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 0 0:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00 :00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=443; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: imp_key=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00 :00:01 GMT; path=/; port=443 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 27-May-2023 05:41:33 GMT; path=/; port=443; secure Connection: close
2022-05-27 05:41:33 UTC	765	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 64 65 22 20 64 69 72 3d 22 6c 74 72 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f Data Ascii: <!DOCTYPE html><html lang="de" dir="ltr"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1"> <meta name="goo
2022-05-27 05:41:33 UTC	771	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 6d 65 73 73 61 67 65 22 3e 54 68 65 20 73 79 73 74 65 6d 20 68 61 73 20 64 65 74 65 63 74 65 64 20 74 68 61 74 20 79 6f 75 20 61 72 65 20 75 73 69 6e 67 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 63 50 61 6e 65 6c 20 26 61 6d 70 3b 20 57 48 4d 20 6e 6f 20 6c 6f 6e 67 65 72 20 73 75 70 70 6f 72 74 73 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 72 65 61 64 20 74 68 65 20 3c 61 20 74 69 74 6c 65 3d 22 63 50 61 6e 65 6c 20 42 6c 6f 67 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6f 2e 63 70 61 6e 65 6c Data Ascii: The system has detected that you are using Internet Explorer 11. cPan el & WHM no longer supports Internet Explorer 11. For more information, read the <a title="cPanel Blog" target="_bla nk" href="https://go.cpanel
2022-05-27 05:41:33 UTC	773	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 22 3e 73 75 6f 6d 69 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 6c 69 70 69 6e 6f 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 Data Ascii: suomi Filipino
2022-05-27 05:41:33 UTC	781	IN	Data Raw: d0 b0 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 76 69 27 3e 54 69 e1 ba bf 6e 67 20 56 69 e1 bb 87 74 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 27 3e e4 b8 ad e6 96 87 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 5f 63 6e 27 3e e4 b8 ad e6 96 87 ef bc 88 e4 b8 ad e5 9b bd ef bc 89 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 5f 74 77 27 3e e4 b8 ad e6 96 87 ef bc 88 e5 8f b0 e6 b9 be ef bc 89 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 64 65 27 3e 44 65 75 74 73 63 68 3c 2f 6f 70 74 69 6f 6e 3e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 73 65 6c 65 63 74 3e 0a 20 Data Ascii: </option><option value='vi'>Ting Vit</option><option value='zh'></option><option value='zh_cn'></option> <option value='zh_tw'></option><option value='de'>Deutsch</option> </select>
2022-05-27 05:41:33 UTC	786	IN	Data Raw: 6f 70 61 63 69 74 79 3d 65 6c 2e 66 69 6c 74 65 72 73 2e 69 74 65 6d 28 22 44 58 49 6d 61 67 65 54 72 61 6e 73 66 6f 72 6d 2e 4d 69 63 72 6f 73 6f 66 74 2e 41 6c 70 68 61 22 29 2e 6f 70 61 63 69 74 79 7d 63 61 74 63 68 28 65 29 7b 74 72 79 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 65 6c 2e 66 69 6c 74 65 72 73 28 22 61 6c 70 68 61 22 29 2e 6f 70 61 63 69 74 79 7d 63 61 74 63 68 28 65 72 72 6f 72 29 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 31 30 30 7d 7d 73 74 61 72 74 5f 6f 70 61 63 69 74 79 2f 3d 31 30 30 7d 69 66 28 21 73 74 61 72 74 5f 6f 70 61 63 69 74 79 29 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 30 7d 7d 65 6c 73 65 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 30 3b 73 65 74 5f 6f 70 61 63 69 74 79 28 65 6c 2c 30 29 7d 69 66 28 5f 66 61 Data Ascii: opacity=el.filters.item("DXImageTransform.Microsoft.Alpha").opacity}catch(e){try{start_opacity=el.filters("a lpha").opacity}catch(error){start_opacity=100}}start_opacity/=100}if(!start_opacity){start_opacity=0}}else{start_opacity =0;set_opacity(el,0)}if(_fa

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:33 UTC	789	IN	Data Raw: 66 3c 74 6f 70 2e 66 72 61 6d 65 73 2e 6c 65 6e 67 74 68 3b 66 2b 2b 29 7b 69 66 28 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 21 3d 3d 77 69 6e 64 6f 77 29 7b 76 61 72 20 68 72 65 66 3d 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 2e 72 65 70 6c 61 63 65 28 2f 5c 2f 63 70 73 65 73 73 5b 2e 5c 64 5d 2b 2f 2c 72 65 73 75 6c 74 2e 73 65 63 75 72 69 74 79 5f 74 6f 6b 65 6e 29 3b 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 68 72 65 66 7d 7d 6c 6f 63 61 74 69 6f 6e 5f 6f 62 6a 5f 74 6f 5f 72 65 64 69 72 65 63 74 3d 6c 6f 63 61 74 69 6f 6e 7d 76 61 72 20 72 65 64 69 72 65 63 74 6f 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 6c 6f 63 61 74 69 6f 6e 5f 6f 62 6a 5f 74 6f 5f 72 65 64 69 72 65 63 Data Ascii: f<top.frames.length;f++){if(top.frames[f]!==window){var href=top.frames[f].location.href.replace(/\/cpsess[.\d]+/,result.security_token);top.frames[f].location.href=href}}}location_obj_to_redirect=location}var redirector=function(){location_obj_to_redirec
2022-05-27 05:41:33 UTC	797	IN	Data Raw: 6b 22 3a 74 2c 22 41 73 69 61 2f 49 72 6b 75 74 73 6b 22 3a 74 2c 22 41 73 69 61 2f 59 61 6b 75 74 73 6b 22 3a 74 2c 22 41 73 69 61 2f 56 6c 61 64 69 76 6f 73 74 6f 6b 22 3a 74 2c 22 41 73 69 61 2f 4b 61 6d 63 68 61 74 6b 61 22 3a 74 2c 22 45 75 72 6f 70 65 2f 4d 69 6e 73 6b 22 3a 74 2c 22 41 75 73 74 72 61 6c 69 61 2f 50 65 72 74 68 22 3a 6e 65 77 20 44 61 74 65 28 32 30 30 38 2c 31 30 2c 31 2c 31 2c 30 2c 30 2c 30 29 7d 3b 72 65 74 75 72 6e 20 6e 5b 65 5d 7d 3b 72 65 74 75 72 6e 7b 64 65 74 65 72 6d 69 6e 65 3a 61 2c 64 61 74 65 5f 69 73 5f 64 73 74 3a 6f 2c 64 73 74 5f 73 74 61 72 74 5f 66 6f 72 3a 66 7d 7d 28 29 3b 74 2e 54 69 6d 65 5a 6f 6e 65 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 6e 3d 7b 22 41 6d Data Ascii: k":t,"Asia/Irkutsk":t,"Asia/Yakutsk":t,"Asia/Vladivostok":t,"Asia/Kamchatka":t,"Europe/Minsk":t,"Australia/Perth":new Date(2008,10,1,1,0,0,0)};return n[e]};return{determine:a,date_is_dst:o,dst_start_for:f}}();t.TimeZone=function(e){"use strict";var n={"Am
2022-05-27 05:41:33 UTC	802	IN	Data Raw: 20 23 73 65 6c 65 63 74 5f 75 73 65 72 5f 66 6f 72 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 70 78 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 70 79 72 69 67 68 74 22 3e 43 6f 70 79 72 69 67 68 74 c2 a9 c2 a0 32 30 32 32 20 63 50 61 6e 65 6c 2c 20 4c 2e 4c 2e 43 2e 0a 20 20 20 20 3c 62 72 20 2f 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6f 2e 63 70 61 6e 65 6c 2e 6e 65 74 2f 70 72 69 76 61 63 79 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 3e 44 61 74 65 6e 73 63 68 75 74 7a 72 69 63 68 74 6c 69 6e 69 65 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 0a 3c 2f 62 6f 64 79 3e 0a 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: #select_user_form { width: px; } }</style> Copyright2022 cPanel, L.L.C. Datenschutzrichtlinie </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49824	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:06 UTC	42	OUT	GET /cPanel_magic_revision_1508464910/unprotected/cpanel/style_v2_optimized.css HTTP/1.1 Host: webmail.unitedyacht.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: style Referer: https://arthurperush.com/css/cPanel.SharePoint_documentOnline/login.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 05:41:07 UTC	43	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:06 GMT Server: Apache/2.4.53 (cPanel) OpenSSL/1.1.1o mod_bwlimited/1.4 Content-Type: text/css Last-Modified: Tue, 17 Aug 2021 02:06:03 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:06 GMT Content-Length: 142431 Vary: Accept-Encoding,User-Agent Connection: close
2022-05-27 05:41:07 UTC	43	IN	Data Raw: 23 70 72 65 6c 6f 61 64 5f 69 6d 61 67 65 73 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 63 50 61 6e 65 6c 5f 6d 61 67 69 63 5f 72 65 76 69 73 69 6f 6e 5f 31 35 34 37 36 36 35 32 38 35 2f 75 6e 70 72 6f 74 65 63 74 65 64 2f 63 70 61 6e 65 6c 2f 69 6d 61 67 65 73 2f 6e 6f 74 69 63 65 2d 65 72 72 6f 72 2e 70 6e 67 29 2c 75 72 6c 28 2f 63 50 61 6e 65 6c 5f 6d 61 67 69 63 5f 72 65 76 69 73 69 6f 6e 5f 31 35 34 37 36 36 35 32 38 35 2f 75 6e 70 72 6f 74 65 63 74 65 64 2f 63 70 61 6e 65 6c 2f 69 6d 61 67 65 73 2f 6e 6f 74 69 63 65 2d 69 6e 66 6f 2e 70 6e 67 29 2c 75 72 6c 28 2f 63 50 61 6e 65 6c 5f 6d 61 67 69 63 5f 72 65 76 69 73 69 6f 6e 5f 31 35 34 37 36 36 35 32 38 35 2f 75 6e 70 72 6f 74 65 63 74 65 64 2f 63 70 61 6e 65 6c 2f 69 6d Data Ascii: #preload_images{background-image:url(/cPanel_magic_revision_1547665285/unprotected/cpanel/images/notice-error.png),url(/cPanel_magic_revision_1547665285/unprotected/cpanel/images/notice-info.png),url(/cPanel_magic_revision_1547665285/unprotected/cpanel/im
2022-05-27 05:41:07 UTC	51	IN	Data Raw: 61 6c 3b 77 69 64 74 68 3a 32 37 34 70 78 7d 40 6d 65 64 69 61 28 6d 69 6e 2d 77 69 64 74 68 3a 34 38 30 70 78 29 7b 23 75 73 65 72 6f 72 6d 20 69 6e 70 75 74 7b 77 69 64 74 68 3a 34 30 30 70 78 7d 7d 40 6d 65 64 69 61 28 6d 69 6e 2d 77 69 64 74 68 3a 31 30 32 34 70 78 29 7b 23 75 73 65 72 66 6f 72 6d 20 69 6e 70 75 74 7b 77 69 64 74 68 3a 36 30 30 70 78 7d 7d 75 6c 2e 76 61 6c 69 64 61 74 69 6f 6e 5f 65 72 72 6f 72 73 5f 75 6c 3e 6c 69 2e 76 61 6c 69 64 61 74 69 6f 6e 5f 65 72 72 6f 72 73 5f 6c 69 7b 6d 61 78 2d 77 69 64 74 68 3a 32 36 30 70 78 7d 40 6d 65 64 69 61 28 6d 69 6e 2d 77 69 64 74 68 3a 34 38 30 70 78 29 7b 75 6c 2e 76 61 6c 69 64 61 74 69 6f 6e 5f 65 72 72 6f 72 73 5f 75 6c 3e 6c 69 2e 76 61 6c 69 64 61 74 69 6f 6e 5f 65 72 72 6f 72 73 5f Data Ascii: al;width:274px}@media(min-width:480px){#userform input{width:400px}}@media(min-width:1024px){#userform input{width:600px}}ul.validation_errors_ul>li.validation_errors_li{max-width:260px}@media(min-width:480px){ul.validation_errors_ul>li.validation_errors_

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:07 UTC	58	IN	Data Raw: 6d 61 78 2d 77 69 64 74 68 3a 35 38 36 70 78 7d 7d 2e 69 6d 61 67 65 2d 77 72 61 70 70 65 72 2c 2e 74 65 78 74 2d 77 72 61 70 70 65 72 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 6d 69 64 64 6c 65 7d 2e 69 6d 61 67 65 2d 77 72 61 70 70 65 72 7b 6d 69 6e 2d 77 69 64 74 68 3a 39 30 70 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 39 30 70 78 7d 2e 62 75 74 74 6f 6e 2d 77 72 61 70 70 65 72 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 66 6c 6f 61 74 3a 6c 65 66 74 7d 2e 62 75 74 74 6f 6e 2d 77 72 61 70 70 65 72 20 62 75 74 74 6f 6e 7b 62 6f 72 64 65 72 3a 30 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 3b 70 61 Data Ascii: max-width:586px}}.image-wrapper,.text-wrapper{display:inline-block;overflow:hidden;vertical-align:middle}.image-wrapper{min-width:90px;min-height:90px}.button-wrapper{display:inline-block;float:left}.button-wrapper button{border:0;background-color:#fff;pa
2022-05-27 05:41:07 UTC	66	IN	Data Raw: 6c 6f 67 69 6e 2d 73 74 61 74 75 73 2d 69 63 6f 6e 2c 23 49 45 2d 77 61 72 6e 69 6e 67 20 2e 49 45 2d 77 61 72 6e 69 6e 67 2d 69 63 6f 6e 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 77 69 64 74 68 3a 32 37 70 78 3b 68 65 69 67 68 74 3a 32 37 70 78 7d 23 6c 6f 67 69 6e 2d 73 74 61 74 75 73 2d 69 63 6f 6e 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 75 72 6c 28 2f 63 50 61 6e 65 6c 5f 6d 61 67 69 63 5f 72 65 76 69 73 69 6f 6e 5f 31 35 34 37 36 36 35 32 38 35 2f 75 6e 70 72 6f 74 65 63 74 65 64 2f 63 70 61 6e 65 6c 2f 69 6d 61 67 65 73 2f 6e 6f 74 69 63 65 2d 65 72 72 6f 72 2e 70 6e 67 29 7d 23 6c 6f 67 69 6e 2d 73 74 61 74 75 73 2e 69 6e 66 6f 2d 6e 6f 74 69 63 65 20 Data Ascii: login-status-icon,#IE-warning .IE-warning-icon{display:block;width:27px;height:27px}#login-status.error-notice .login-status-icon{background-image:url(/cPanel_magic_revision_1547665285/unprotected/cpanel/images/notice-error.png)}#login-status.info-notice
2022-05-27 05:41:07 UTC	73	IN	Data Raw: 7d 68 74 6d 6c 5b 64 69 72 3d 22 72 74 6c 22 5d 20 23 72 65 73 65 74 5f 66 6f 72 6d 20 2e 69 6e 70 75 74 2d 67 72 6f 75 70 20 69 6e 70 75 74 2e 73 74 64 5f 74 65 78 74 62 6f 78 2c 68 74 6d 6c 5b 64 69 72 3d 22 72 74 6c 22 5d 20 2e 69 6e 70 75 74 2d 66 69 65 6c 64 2d 6c 6f 67 69 6e 2e 69 63 6f 6e 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 70 6f 73 69 74 69 6f 6e 3a 72 69 67 68 74 7d 2e 69 6e 70 75 74 2d 62 75 74 74 6f 6e 7b 77 69 64 74 68 3a 32 38 30 70 78 7d 69 6e 70 75 74 2e 73 74 64 5f 74 65 78 74 62 6f 78 7b 68 65 69 67 68 74 3a 32 39 70 78 3b 6d 69 6e 2d 77 69 64 74 68 3a 32 32 30 70 78 7d 68 74 6d 6c 5b 64 69 72 3d 22 72 74 6c 22 5d 20 23 72 65 73 65 74 5f 66 6f 72 6d 20 2e 69 6e 70 75 74 2d 67 72 6f 75 70 20 69 6e 70 75 74 2e 73 74 64 5f 74 65 78 74 62 6f Data Ascii: }html[dir="rtl"] #reset_form .input-group input.std_textbox,html[dir="rtl"] .input-field-login.icon{background-position:right}.input-button{width:280px}input.std_textbox{height:29px;min-width:220px}html[dir="rtl"] #reset_form .input-group input.std_textbo
2022-05-27 05:41:07 UTC	74	IN	Data Raw: 61 64 64 69 6e 67 3a 30 7d 23 6c 6f 63 61 6c 65 2d 63 6f 6e 74 61 69 6e 65 72 7b 77 69 64 74 68 3a 31 30 30 25 3b 68 65 69 67 68 74 3a 61 75 74 6f 3b 6d 69 6e 2d 77 69 64 74 68 3a 32 38 30 70 78 3b 6d 61 72 67 69 6e 3a 31 35 70 78 20 30 3b 63 6f 6c 6f 72 3a 23 32 39 33 61 34 61 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 4f 70 65 6e 20 53 61 6e 73 22 2c 73 61 6e 73 2d 73 65 72 69 66 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 36 30 30 3b 70 61 64 64 69 6e 67 3a 30 7d 23 6c 6f 63 61 6c 65 2d 63 6f 6e 74 61 69 6e 65 72 20 61 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 64 30 33 66 30 30 7d 23 6c 6f 63 61 6c 65 2d 6d 61 70 20 2e 73 63 72 6f 6c 6c 65 72 7b 6d 61 78 2d 68 65 69 67 68 74 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 3a 30 7d 23 6c 6f 63 61 6c 65 2d 68 65 61 64 Data Ascii: adding:0}#locale-container{width:100%;height:auto;min-width:280px;margin:15px 0;color:#293a4a;font-family:"Open Sans",sans-serif;font-weight:600;padding:0}#locale-container a:hover{color:#d03f00}#locale-map .scroller{max-height:none;padding:0}#locale-head
2022-05-27 05:41:07 UTC	82	IN	Data Raw: 6f 6e 74 65 6e 74 3a 22 5c 66 30 34 32 22 7d 2e 66 61 2d 61 64 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 37 30 22 7d 2e 66 61 2d 61 64 6f 62 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 37 37 38 22 7d 2e 66 61 2d 61 64 76 65 72 73 61 6c 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 33 36 61 22 7d 2e 66 61 2d 61 66 66 69 6c 69 61 74 65 74 68 65 6d 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 33 36 62 22 7d 2e 66 61 2d 61 69 72 2d 66 72 65 73 68 65 6e 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 35 64 30 22 7d 2e 66 61 2d 61 69 72 62 6e 62 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 38 33 34 22 7d 2e 66 61 2d 61 6c 67 6f 6c 69 61 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 Data Ascii: ontent:"\f042"}.fa-adn:before{content:"\f170"}.fa-adobe:before{content:"\f778"}.fa-adversal:before{content:"\f36a"}.fa-affiliatetheme:before{content:"\f36b"}.fa-air-freshener:before{content:"\f5d0"}.fa-airbnb:before{content:"\f834"}.fa-algolia:before{cont
2022-05-27 05:41:07 UTC	89	IN	Data Raw: 73 71 75 61 72 65 2d 6c 65 66 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 39 31 22 7d 2e 66 61 2d 63 61 72 65 74 2d 73 71 75 61 72 65 2d 72 69 67 68 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 35 32 22 7d 2e 66 61 2d 63 61 72 65 74 2d 73 71 75 61 72 65 2d 75 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 35 31 22 7d 2e 66 61 2d 63 61 72 65 74 2d 75 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 64 38 22 7d 2e 66 61 2d 63 61 72 72 6f 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 37 38 37 22 7d 2e 66 61 2d 63 61 72 74 2d 61 72 72 6f 77 2d 64 6f 77 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 31 38 22 7d 2e 66 61 2d 63 61 72 74 2d 70 6c 75 73 3a 62 65 66 6f Data Ascii: square-left:before{content:"\f191"}.fa-caret-square-right:before{content:"\f152"}.fa-caret-square-up:before{content:"\f151"}.fa-caret-up:before{content:"\f0d8"}.fa-carrot:before{content:"\f787"}.fa-cart-arrow-down:before{content:"\f218"}.fa-cart-plus:befo
2022-05-27 05:41:07 UTC	90	IN	Data Raw: 6b 2d 63 69 72 63 6c 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 35 38 22 7d 2e 66 61 2d 63 68 65 63 6b 2d 64 6f 75 62 6c 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 35 36 30 22 7d 2e 66 61 2d 63 68 65 63 6b 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 34 61 22 7d 2e 66 61 2d 63 68 65 65 73 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 37 65 66 22 7d 2e 66 61 2d 63 68 65 73 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 34 33 39 22 7d 2e 66 61 2d 63 68 65 73 73 2d 62 69 73 68 6f 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 34 33 61 22 7d 2e 66 61 2d 63 68 65 73 73 2d 62 6f 61 72 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 34 33 Data Ascii: k-circle:before{content:"\f058"}.fa-check-double:before{content:"\f560"}.fa-check-square:before{content:"\f14a"}.fa-cheese:before{content:"\f7ef"}.fa-chess:before{content:"\f439"}.fa-chess-bishop:before{content:"\f43a"}.fa-chess-board:before{content:"\f43
2022-05-27 05:41:07 UTC	98	IN	Data Raw: 6e 74 3a 22 5c 66 30 34 39 22 7d 2e 66 61 2d 66 61 73 74 2d 66 6f 72 77 61 72 64 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 35 30 22 7d 2e 66 61 2d 66 61 78 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 61 63 22 7d 2e 66 61 2d 66 65 61 74 68 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 35 32 64 22 7d 2e 66 61 2d 66 65 61 74 68 65 72 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 35 36 62 22 7d 2e 66 61 2d 66 65 64 65 78 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 37 39 37 22 7d 2e 66 61 2d 66 65 64 6f 72 61 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 37 39 38 22 7d 2e 66 61 2d 66 65 6d 61 6c 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 38 32 Data Ascii: nt:"\f049"}.fa-fast-forward:before{content:"\f050"}.fa-fax:before{content:"\f1ac"}.fa-feather:before{content:"\f52d"}.fa-feather-alt:before{content:"\f56b"}.fa-fedex:before{content:"\f797"}.fa-fedora:before{content:"\f798"}.fa-female:before{content:"\f182

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:07 UTC	104	IN	Data Raw: 74 65 6e 74 3a 22 5c 66 32 35 37 22 7d 2e 66 61 2d 68 61 6e 64 2d 73 70 6f 63 6b 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 35 39 22 7d 2e 66 61 2d 68 61 6e 64 73 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 34 63 32 22 7d 2e 66 61 2d 68 61 6e 64 73 2d 68 65 6c 70 69 6e 67 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 34 63 34 22 7d 2e 66 61 2d 68 61 6e 64 73 68 61 6b 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 62 35 22 7d 2e 66 61 2d 68 61 6e 75 6b 69 61 68 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 36 65 36 22 7d 2e 66 61 2d 68 61 72 64 2d 68 61 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 38 30 37 22 7d 2e 66 61 2d 68 61 73 68 74 61 67 3a 62 65 66 6f 72 65 7b 63 6f Data Ascii: tent:"\f257"}.fa-hand-spock:before{content:"\f259"}.fa-hands:before{content:"\f4c2"}.fa-hands-helping:before{content:"\f4c4"}.fa-handshake:before{content:"\f2b5"}.fa-hanukiah:before{content:"\f6e6"}.fa-hard-hat:before{content:"\f807"}.fa-hashtag:before{co
2022-05-27 05:41:07 UTC	106	IN	Data Raw: 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 35 32 22 7d 2e 66 61 2d 68 6f 75 72 67 6c 61 73 73 2d 73 74 61 72 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 35 31 22 7d 2e 66 61 2d 68 6f 75 73 65 2d 64 61 6d 61 67 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 36 66 31 22 7d 2e 66 61 2d 68 6f 75 7a 7a 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 37 63 22 7d 2e 66 61 2d 68 72 79 76 6e 69 61 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 36 66 32 22 7d 2e 66 61 2d 68 74 6d 6c 35 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 33 62 22 7d 2e 66 61 2d 68 75 62 73 70 6f 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 33 62 32 22 7d 2e 66 61 2d 69 2d 63 75 72 73 6f 72 3a 62 65 66 6f 72 65 7b Data Ascii: content:"\f252"}.fa-hourglass-start:before{content:"\f251"}.fa-house-damage:before{content:"\f6f1"}.fa-houzz:before{content:"\f27c"}.fa-hryvnia:before{content:"\f6f2"}.fa-html5:before{content:"\f13b"}.fa-hubspot:before{content:"\f3b2"}.fa-i-cursor:before{
2022-05-27 05:41:07 UTC	114	IN	Data Raw: 31 62 30 22 7d 2e 66 61 2d 70 61 79 70 61 6c 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 65 64 22 7d 2e 66 61 2d 70 65 61 63 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 36 37 63 22 7d 2e 66 61 2d 70 65 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 33 30 34 22 7d 2e 66 61 2d 70 65 6e 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 33 30 35 22 7d 2e 66 61 2d 70 65 6e 2d 66 61 6e 63 79 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 35 61 63 22 7d 2e 66 61 2d 70 65 6e 2d 6e 69 62 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 35 61 64 22 7d 2e 66 61 2d 70 65 6e 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 34 62 22 7d 2e 66 61 2d 70 65 6e Data Ascii: 1b0"}.fa-paypal:before{content:"\f1ed"}.fa-peace:before{content:"\f67c"}.fa-pen:before{content:"\f304"}.fa-pen-alt:before{content:"\f305"}.fa-pen-fancy:before{content:"\f5ac"}.fa-pen-nib:before{content:"\f5ad"}.fa-pen-square:before{content:"\f14b"}.fa-pen
2022-05-27 05:41:07 UTC	120	IN	Data Raw: 61 22 7d 2e 66 61 2d 73 68 6f 70 77 61 72 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 35 62 35 22 7d 2e 66 61 2d 73 68 6f 77 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 63 63 22 7d 2e 66 61 2d 73 68 6f 72 74 73 74 6c 65 2d 76 61 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 35 62 36 22 7d 2e 66 61 2d 73 69 67 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 34 64 39 22 7d 2e 66 61 2d 73 69 67 6e 2d 69 6e 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 66 36 22 7d 2e 66 61 2d 73 69 67 6e 2d 6c 61 6e 67 75 61 67 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 61 37 22 7d 2e 66 61 2d 73 69 67 6e 2d 6f 75 74 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 Data Ascii: a"}.fa-shopware:before{content:"\f5b5"}.fa-shower:before{content:"\f2cc"}.fa-shuttle-van:before{content:"\f5b6"}.fa-sign:before{content:"\f4d9"}.fa-sign-in-alt:before{content:"\f2f6"}.fa-sign-language:before{content:"\f2a7"}.fa-sign-out-alt:before{content
2022-05-27 05:41:07 UTC	122	IN	Data Raw: 74 2d 75 70 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 38 38 35 22 7d 2e 66 61 2d 73 6f 72 74 2d 64 6f 77 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 64 64 22 7d 2e 66 61 2d 73 6f 72 74 2d 6e 75 6d 65 72 69 63 2d 64 6f 77 6e 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 36 32 22 7d 2e 66 61 2d 73 6f 72 74 2d 6e 75 6d 65 72 69 63 2d 64 6f 77 6e 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 38 38 36 22 7d 2e 66 61 2d 73 6f 72 74 2d 6e 75 6d 65 72 69 63 2d 75 70 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 36 33 22 7d 2e 66 61 2d 73 6f 72 74 2d 6e 75 6d 65 72 69 63 2d 75 70 2d 61 6c 74 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 38 38 37 22 7d 2e 66 Data Ascii: t-up-alt:before{content:"\f885"}.fa-sort-down:before{content:"\f0dd"}.fa-sort-numeric-down:before{content:"\f162"}.fa-sort-numeric-down-alt:before{content:"\f886"}.fa-sort-numeric-up:before{content:"\f163"}.fa-sort-numeric-up-alt:before{content:"\f887"}.f
2022-05-27 05:41:07 UTC	130	IN	Data Raw: 61 2d 76 69 62 65 72 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 34 30 39 22 7d 2e 66 61 2d 76 69 64 65 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 30 33 64 22 7d 2e 66 61 2d 76 69 64 65 6f 2d 73 6c 61 73 68 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 34 65 32 22 7d 2e 66 61 2d 76 69 68 61 72 61 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 36 61 37 22 7d 2e 66 61 2d 76 69 6d 65 6f 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 34 30 61 22 7d 2e 66 61 2d 76 69 6d 65 6f 2d 73 71 75 61 72 65 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 31 39 34 22 7d 2e 66 61 2d 76 69 6d 65 6f 2d 76 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 5c 66 32 37 64 22 7d 2e 66 61 2d 76 69 6e 65 3a 62 Data Ascii: a-viber:before{content:"\f409"}.fa-video:before{content:"\f03d"}.fa-video-slash:before{content:"\f4e2"}.fa-vihara:before{content:"\f6a7"}.fa-vimeo:before{content:"\f40a"}.fa-vimeo-square:before{content:"\f194"}.fa-vimeo-v:before{content:"\f27d"}.fa-vine:b
2022-05-27 05:41:07 UTC	136	IN	Data Raw: 6e 67 74 68 2d 32 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 30 7d 75 6c 2e 73 74 72 65 6e 67 74 68 20 2e 73 74 72 65 6e 67 74 68 2d 33 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 39 66 30 7d 75 6c 2e 73 74 72 65 6e 67 74 68 20 2e 73 74 72 65 6e 67 74 68 2d 34 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 30 66 30 7d 2e 67 72 6f 77 6c 2d 63 6f 6e 74 61 69 6e 65 72 2e 67 72 6f 77 6c 2d 66 69 78 65 64 7b 70 6f 73 69 74 69 6f 6e 3a 66 69 78 65 64 3b 66 6c 6f 61 74 3a 72 69 67 68 74 3b 77 69 64 74 68 3a 39 30 25 3b 6d 61 78 2d 77 69 64 74 68 3a 34 30 30 70 78 3b 7a 2d 69 6e 64 65 78 3a 39 39 39 39 7d 2e 67 72 6f 77 6c 2d 63 6f 6e 74 61 69 6e 65 72 2e 67 72 6f 77 6c 2d 66 69 78 65 64 2e 74 6f 70 2d 72 69 67 68 74 7b Data Ascii: ngth-2{background-color:#ff0}ul.strength .strength-3{background-color:#9f0}ul.strength .strength-4{background-color:#0f0}.growl-container.growl-fixed{position:fixed;float:right;width:90%;max-width:400px;z-index:9999}.growl-container.growl-fixed.top-right{
2022-05-27 05:41:07 UTC	138	IN	Data Raw: 48 43 41 41 41 52 4b 43 42 4b 72 42 42 47 2f 54 42 47 43 7a 41 42 68 7a 42 42 64 7a 42 43 2f 78 67 4e 6f 52 43 4a 4d 54 43 51 68 42 43 43 6d 53 41 48 48 4a 67 4b 61 79 43 51 69 69 47 7a 62 41 64 4b 6d 41 76 31 45 41 64 4e 4d 42 52 61 49 61 54 63 41 34 75 77 6c 57 34 44 6a 31 77 44 2f 70 68 43 4a 37 42 4b 4c 79 42 43 51 52 42 79 41 67 54 59 53 48 61 69 41 46 69 69 6c 67 6a 6a 67 67 58 6d 59 58 34 49 63 46 49 42 42 4b 4c 4a 43 44 4a 69 42 52 52 49 6b 75 52 4e 55 67 78 55 6f 70 55 49 46 56 49 48 66 49 39 63 67 49 35 68 31 78 47 75 70 45 37 79 41 41 79 67 76 79 47 76 45 63 78 6c 49 47 79 55 54 33 55 44 4c 56 44 75 61 67 33 47 6f 52 47 6f 67 76 51 5a 48 51 78 6d 6f 38 57 6f 4a 76 51 63 72 51 61 50 59 77 32 6f 65 66 51 71 32 67 50 32 6f 38 2b 51 38 63 77 77 4f Data Ascii: HCAAARKCBKrBBG/TBGCzABhzBBdzBC/xgNoRCJMTCQhBCCmSAHHJgKayCQiiGzbAdKmAv1EAdNMBRaIaTcA4uwlW4Dj1wD/phCJ7BKLyBCQRByAgTYSHaiAFiilgjjggXmYX4IcFIBBKLJCDJiBRRIkuRNUgxUopUIFVIHfl9cgI5h1xGupE7yAAygvyGvEcxlIGyUT3UDLVDuag3GoRGogvQZHQxmo8WoJvQcrQaPYw2oefQq2gP2o8+Q8cwwO

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:07 UTC	146	IN	Data Raw: 38 7a 71 68 71 73 63 30 6d 69 65 5a 4f 62 2b 62 66 68 77 61 6d 76 32 31 73 48 44 6c 58 37 35 2f 76 63 55 53 75 44 77 2b 66 6a 72 64 54 62 4f 69 56 52 6b 4d 39 39 49 6c 66 68 4a 4a 55 52 53 30 44 51 32 33 44 2f 57 69 74 43 78 4f 70 37 66 55 61 76 31 79 31 4f 62 69 6d 70 71 51 71 62 33 39 6c 63 46 6d 2b 79 4c 44 4d 4f 34 6f 6d 2f 4c 57 31 6d 57 4c 79 37 57 63 46 77 41 41 6f 4b 36 73 76 4b 62 55 36 39 6e 63 79 4d 70 61 57 73 35 64 47 42 6a 6f 74 51 38 50 4e 78 74 73 74 76 65 35 2b 7a 43 4e 4a 6b 6b 59 6a 62 65 4f 37 4b 5a 38 6d 5a 33 4f 6e 51 71 37 2f 57 46 57 35 53 59 53 77 46 42 55 4e 77 44 41 39 2b 6c 70 4d 72 71 31 64 5a 36 2f 72 69 44 4a 6c 4b 6d 74 37 62 72 5a 36 64 77 35 64 4f 6e 35 6e 73 78 50 49 79 4f 76 4e 32 64 6e 62 32 53 56 76 31 37 50 4d 70 47 Data Ascii: 8zqhqsc0mieZOb+bfhwamv21sHDlX75/vcUSuDw+fjrdTbOiVRkM99IlfhJJURS0DQ23D/WitCxOp7fUav1y1Obi mpqQqb39lcFm+yLDMO4om/LW1mWLy7WcFwAAoK6svKbU69ncyMpaWs5dGBjotQ8PNxtstve5+zCNJkkYjbeO7KZ8mZ 3OnQq7/WFW5SYSwFBUNwDA9+lpMrq1dZ6/riDJlKmt7brZ6dw5dOn5nsxPIyOvN2dnb2SVv17PMpG
2022-05-27 05:41:07 UTC	152	IN	Data Raw: 68 64 59 77 50 32 53 79 63 51 57 48 54 41 34 76 63 41 41 50 4b 37 62 38 48 55 4b 41 67 44 67 47 69 44 34 63 39 33 2f 2b 38 2f 55 65 67 4a 51 43 41 5a 6b 6d 53 63 51 41 41 58 6b 51 6b 4c 6c 54 4b 73 7a 2f 48 43 41 41 41 52 4b 43 42 4b 72 42 42 47 2f 54 42 47 43 7a 41 42 68 7a 42 42 64 7a 42 43 2f 78 67 4e 6f 52 43 4a 4d 54 43 51 68 42 43 43 6d 53 41 48 48 4a 67 4b 61 79 43 51 69 69 47 7a 62 41 64 4b 6d 41 76 31 45 41 64 4e 4d 42 52 61 49 61 54 63 41 34 75 77 6c 57 34 44 6a 31 77 44 2f 70 68 43 4a 37 42 4b 4c 79 42 43 51 52 42 79 41 67 54 59 53 48 61 69 41 46 69 69 6c 67 6a 6a 67 67 58 6d 59 58 34 49 63 46 49 42 42 4b 4c 4a 43 44 4a 69 42 52 52 49 6b 75 52 4e 55 67 78 55 6f 70 55 49 46 56 49 48 66 49 39 63 67 49 35 68 31 78 47 75 70 45 37 79 41 41 79 67 76 Data Ascii: hdYwP2SycQWHTA4vcAAPK7b8HUKAgDgGiD4c93/+8/UegJQCAZkmScQAAXkQkLlTKsz/HCAAARKCBK rBBG/TBGCzABhzBBdzBC/xgNoRCJMTCQhBCCmSAHHJgKayCQiiGzbAdKmAv1EAdNMBRaIaTcA4uwlW4D j1wD/phCJ7BKLyBCQRByAgTYSHaiAFiilgjjggXmYX4IcFIBBKLJCDJiBRRIkuRNUgxUopUIFVIHfI9cgI5h1xGupE7yAAygv
2022-05-27 05:41:07 UTC	154	IN	Data Raw: 37 30 56 76 76 74 77 58 66 63 64 78 33 76 6f 39 38 50 54 2b 52 38 49 48 38 6f 2f 32 6a 35 73 66 56 54 30 4b 66 37 6b 78 6d 54 6b 2f 38 45 41 35 6a 7a 2f 47 4d 7a 4c 64 73 41 41 41 41 67 59 30 68 53 54 51 41 41 65 69 55 41 41 49 43 44 41 41 44 35 2f 77 41 41 67 4f 6b 41 41 48 55 77 41 41 44 71 59 41 41 41 4f 70 67 41 41 42 64 76 6b 6c 2f 46 52 67 41 41 41 64 68 4a 52 45 46 55 65 4e 72 55 6c 72 39 4c 49 30 45 55 78 7a 39 52 69 78 52 58 57 4f 62 51 77 73 4b 41 64 68 4a 6b 73 41 6a 59 57 6c 70 61 65 42 67 59 41 79 63 69 4b 43 68 33 42 7a 72 43 67 4d 52 66 34 46 6d 6c 38 41 62 73 39 4f 44 2b 67 65 75 30 6b 31 47 49 6e 51 63 70 7a 69 4c 43 46 58 74 67 6b 57 4b 4c 51 43 78 38 51 74 6a 4c 48 71 74 47 30 41 66 44 73 75 2f 74 7a 4a 76 76 39 2f 76 65 7a 4b 61 61 7a Data Ascii: 70VvvtwXfcdx3vo98PT+R8IH8o/2j5sfVT0Kf7kxmTk/8EA5jz/GMzLdsAAAAgY0hSTQAAeiUAAICD AAD5/wAAgOkAAHUwAADqYAAAOpgAABdvkl/FRgAAAdhJREFUeNrUlr9LI0EUxz9RixRXWObQwsKAdhJksAjYWlpaeB gYAyciKCh3BzrCgMRf4Fml8Abs9OD+geu0k1GInQcpziLCFXtgkWKLQCx8QtjLHqtG0AfDsu/tzJvv9/vezKaaz
2022-05-27 05:41:07 UTC	162	IN	Data Raw: 6c 65 72 74 2d 64 61 6e 67 65 72 20 2e 61 6c 65 72 74 2d 6d 65 73 73 61 67 65 20 75 6c 20 6c 69 3e 2a 7b 63 6f 6c 6f 72 3a 23 33 33 33 7d 2e 61 6c 65 72 74 20 2e 62 74 6e 2d 6d 6f 72 65 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 30 7d 5b 64 69 72 3d 22 6c 74 72 22 5d 20 62 6f 64 79 2e 77 68 6f 73 74 6d 61 69 6c 2d 6c 69 73 74 20 2e 61 6c 65 72 74 2d 6d 65 73 73 61 67 65 2c 5b 64 69 72 3d 22 72 74 6c 22 5d 20 62 6f 64 79 2e 77 68 6f 73 74 6d 67 72 20 2e 61 6c 65 72 74 2d 6c 69 73 74 20 2e 61 6c 65 72 74 2d 6d 65 73 73 61 67 65 7b 6d 61 72 67 69 6e 3a 30 7d 5b 64 69 72 3d 22 6c 74 72 22 5d 20 62 6f 64 79 2e 77 68 6f 73 74 6d 67 72 20 2e 61 6c 65 72 74 2d 6c 69 73 74 20 2e 61 6c 65 72 74 2d 6d 65 73 73 61 67 65 3e 2e 61 6c 65 72 74 2d 74 69 74 Data Ascii: lert-danger .alert-message ul li>*{color:#333}.alert .btn-more{padding-top:0}[dir="ltr"] body.whostmgr .alert-list .alert-message,[dir="rtl"] body.whostmgr .alert-list .alert-message{margin:0}[dir="ltr"] body.whostmgr .alert-list .alert-m essage>.alert-tit
2022-05-27 05:41:07 UTC	167	IN	Data Raw: 65 72 74 2d 6c 69 73 74 2d 63 6f 6e 74 61 69 6e 65 72 2e 70 6f 73 69 74 69 6f 6e 2d 74 6f 70 2d 6d 69 64 64 6c 65 2e 73 68 6f 77 2d 73 63 72 6f 6c 6c 2d 62 61 72 7b 6f 76 65 72 66 6c 6f 77 2d 79 3a 73 63 72 6f 6c 6c 7d 2e 77 68 6f 73 74 6d 67 72 20 2e 61 6c 65 72 74 2d 6c 69 73 74 2d 63 6f 6e 74 61 69 6e 65 72 2e 70 6f 73 69 74 69 6f 6e 2d 74 6f 70 2d 6d 69 64 64 6c 65 7b 74 6f 70 3a 37 30 70 78 7d 2e 63 70 61 6e 65 6c 5f 62 6f 64 79 20 2e 61 6c 65 72 74 2d 6c 69 73 74 2d 63 6f 6e 74 61 69 6e 65 72 2e 70 6f 73 69 74 69 6f 6e 2d 74 6f 70 2d 6d 69 64 64 6c 65 7b 74 6f 70 3a 33 30 70 78 7d 2e 77 65 62 6d 61 69 6c 20 2e 61 6c 65 72 74 2d 6c 69 73 74 2d 63 6f 6e 74 61 69 6e 65 72 2e 70 6f 73 69 74 69 6f 6e 2d 74 6f 70 2d 6d 69 64 64 6c 65 7b 74 6f 70 3a 35 32 Data Ascii: ert-list-container.position-top-middle.show-scroll-bar{overflow-y:scroll}.whostmgr .alert-list-container.position-top-middle{top:70px}.cpanel_body .alert-list-container.position-top-middle{top:30px}.webmail .alert-list-container.position-top-middle{top:52
2022-05-27 05:41:07 UTC	170	IN	Data Raw: 74 2d 6c 69 73 74 7b 77 69 64 74 68 3a 31 30 30 25 7d 40 6d 65 64 69 61 28 6d 69 6e 2d 77 69 64 74 68 3a 37 36 38 70 78 29 7b 2e 61 6c 65 72 74 2d 6c 69 73 74 2d 63 6f 6e 74 61 69 6e 65 72 2e 70 6f 73 69 74 69 6f 6e 2d 6d 69 64 64 6c 65 2d 6c 65 66 74 20 2e 61 6c 65 72 74 2d 6c 69 73 74 7b 6d 61 78 2d 77 69 64 74 68 3a 35 30 30 70 78 7d 7d 2e 61 6c 65 72 74 2d 6c 69 73 74 2d 63 6f 6e 74 61 69 6e 65 72 2e 70 6f 73 69 74 69 6f 6e 2d 6d 69 64 64 6c 65 2d 6c 65 66 74 2e 73 68 6f 77 2d 73 63 72 6f 6c 6c 2d 62 61 72 7b 6f 76 65 72 66 6c 6f 77 2d 79 3a 73 63 72 6f 6c 6c 7d 2e 61 6c 65 72 74 2d 6c 69 73 74 2d 63 6f 6e 74 61 69 6e 65 72 2e 70 6f 73 69 74 69 6f 6e 2d 6d 69 64 64 6c 65 2d 6c 65 66 74 20 2e 61 6c 65 72 74 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 31 70 78 Data Ascii: t-list{width:100%}@media(min-width:768px){.alert-list-container.position-middle-left .alert-list{max-width:5 00px}}.alert-list-container.position-middle-left.show-scroll-bar{overflow-y:scroll}.alert-list-container.position-middle-left .ale rt{margin-top:1px
2022-05-27 05:41:07 UTC	178	IN	Data Raw: 6d 61 74 65 20 2a 7b 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 69 74 69 6f 6e 3a 6e 6f 6e 65 21 69 6d 70 6f 72 74 61 6e 74 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 6e 6f 6e 65 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 75 73 65 72 2d 64 6f 6d 61 69 6e 2d 6c 69 73 74 2d 64 69 72 65 63 74 69 76 65 20 2e 6e 6f 2d 72 65 73 75 6c 74 73 2d 6d 73 67 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 7d 2e 75 73 65 72 2d 64 6f 6d 61 69 6e 2d 6c 69 73 74 2d 64 69 72 65 63 74 69 76 65 20 2e 66 69 78 65 64 2d 77 69 64 74 68 2d 74 61 62 6c 65 7b 74 61 62 6c 65 2d 6c 61 79 6f 75 74 3a 66 69 78 65 64 7d 2e 75 73 65 72 2d 64 6f 6d 61 69 6e 2d 6c 69 73 74 2d 64 69 72 65 63 74 69 76 65 20 2e 65 64 69 74 2d 6c 6f 63 6b 65 64 7b 66 6f 6e 74 2d 73 74 79 6c 65 3a 69 74 61 6c 69 63 3b 70 6f 69 6e 74 65 Data Ascii: mate *{-webkit-transition:none!important;transition:none!important}.user-domain-list-directive .no-results-m sg{margin-top:0}.user-domain-list-directive .fixed-width-table{table-layout:fixed}.user-domain-list-directive .edit-locked{font-style:italic;pointe
2022-05-27 05:41:07 UTC	183	IN	Data Raw: 69 64 20 23 64 64 64 7d 2e 73 74 61 74 73 2d 77 69 64 67 65 74 20 68 74 6d 6c 5b 64 69 72 3d 22 72 74 6c 22 5d 20 2e 73 74 61 74 73 2d 77 69 64 67 65 74 2d 66 6f 6f 74 65 72 20 61 3a 6e 6f 74 28 3a 66 69 72 73 74 2d 63 68 69 6c 64 29 7b 62 6f 72 64 65 72 2d 72 69 67 68 74 3a 31 70 78 20 73 6f 6c 69 64 20 23 64 64 64 7d 68 74 6d 6c 5b 64 61 74 61 2d 73 74 79 6c 65 3d 22 64 61 72 6b 22 5d 20 2e 73 74 61 74 73 2d 77 69 64 67 65 74 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 32 32 32 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 6e 6f 6e 65 3b 62 6f 72 64 65 72 3a 31 70 78 20 73 6f 6c 69 64 20 23 31 64 31 64 31 64 3b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 33 70 78 7d 68 74 6d 6c 5b 64 61 74 61 2d 73 74 79 Data Ascii: id #ddd}.stats-widget html[dir="rtl"] .stats-widget-footer a:not(:first-child){border-right:1px solid #ddd}html[data-style="dark"] .stats-widget{background-color:#222;margin-top:20px;box-shadow:none;border:1px solid #1d1d1d;border-radius:3px}html[data-sty

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:07 UTC	186	IN	Data Raw: 70 61 6e 65 6c 2f 69 6d 61 67 65 73 2f 69 63 6f 6e 2d 70 61 73 73 77 6f 72 64 2e 70 6e 67 29 3b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 68 65 69 67 68 74 3a 33 34 70 78 3b 77 69 64 74 68 3a 31 30 30 25 3b 6d 61 72 67 69 6e 3a 30 7d 23 72 65 73 65 74 5f 66 6f 72 6d 20 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 62 74 6e 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 77 69 64 74 68 3a 31 30 30 25 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 64 64 64 3b 62 6f 72 64 65 72 3a 32 70 78 20 73 6f 6c 69 64 20 23 62 65 62 65 62 65 3b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 30 20 30 20 34 70 78 20 34 70 78 3b 62 6f 72 64 65 72 2d 74 Data Ascii: panel/images/icon-password.png);box-sizing:border-box;height:34px;width:100%;margin:0}#reset_form .input-group-btn{box-sizing:border-box;display:block;width:100%;text-align:center;background:#ddd;border:2px solid #bebebe;border-radius:0 0 4px 4px;border-t

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49956	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:34 UTC	802	OUT	GET /?locale=el HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: roundcube_cookies=enabled; timezone=America/Los_Angeles; webmailsession=%3aZEm_sI1rJvNEi7by%2c4ab193791d9e20fba6816ee2acc3df28; session_locale=de
2022-05-27 05:41:35 UTC	803	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:35 GMT Server: Apache Content-Type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 38890 Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: webmailsession=%3atv2V2gFhVsVxQnAL%2ca29dc2d32ccadd90323922aa2d946414; HttpOnly; path=/; port=443; secure Set-Cookie: session_locale=el; expires=Sat, 27-May-2023 05:41:35 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=443; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: imp_key=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 27-May-2023 05:41:35 GMT; path=/; port=443; secure Connection: close
2022-05-27 05:41:35 UTC	805	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6c 22 20 64 69 72 3d 22 6c 74 72 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f Data Ascii: <!DOCTYPE html><html lang="el" dir="ltr"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1"> <meta name="goo

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:35 UTC	811	IN	Data Raw: 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 65 6e 74 2d 77 72 61 70 70 65 72 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 64 65 74 61 69 6c 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 69 63 6f 6e 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 69 63 6f 6e 22 3e 3c 2f 73 70 61 6e 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 6d 65 73 73 61 67 65 22 3e 54 68 65 20 73 79 73 74 65 6d 20 68 61 73 20 64 65 74 65 63 74 65 64 20 74 Data Ascii: <div class="content-wrapper"> <div id="IE-warning-detail"> <div id="IE-warning-icon-container"></div> <div id="IE-warning-message">The system has detected t
2022-05-27 05:41:35 UTC	813	IN	Data Raw: 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 65 73 5f 34 31 39 22 3e 65 73 70 61 c3 b1 6f 6c 20 6c 61 74 69 6e 6f 61 6d 65 72 69 63 61 6e 6f 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 65 73 5f 65 73 22 3e 65 73 70 61 c3 b1 6f 6c 20 64 65 20 45 73 70 61 c3 b1 61 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 Data Ascii: >espaol latinoamericano</div> <div class="locale-cell">espaol de Espaa</div> <div clas
2022-05-27 05:41:35 UTC	821	IN	Data Raw: 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 70 74 5f 62 72 27 3e 70 6f 72 74 75 67 75 c3 aa 73 20 64 6f 20 42 72 61 73 69 6c 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 72 6f 27 3e 72 6f 6d c3 a2 6e c4 83 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 72 75 27 3e d1 80 d1 83 d1 81 d1 81 d0 ba d0 b8 d0 b9 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 73 6c 27 3e 73 6c 6f 76 65 6e c5 a1 c4 8d 69 6e 61 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 73 76 27 3e 73 76 65 6e 73 6b 61 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 74 68 27 3e e0 b9 84 e0 b8 97 e0 b8 a2 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f Data Ascii: option><option value='pt_br'>portugus do Brasil</option><option value='ro'>romn</option><option value='ru'></option><option value='sl'>slovenina</option><option value='sv'>svenska</option><option value='th'></option><optio
2022-05-27 05:41:35 UTC	826	IN	Data Raw: 73 68 6f 77 5f 6c 6f 63 61 6c 65 73 3f 66 61 64 65 5f 6f 75 74 3a 66 61 64 65 5f 69 6e 29 28 22 6c 6f 63 61 6c 65 2d 66 6f 6f 74 65 72 22 29 29 7d 66 75 6e 63 74 69 6f 6e 20 73 68 6f 77 49 45 42 61 6e 6e 65 72 28 29 7b 69 66 28 6e 61 76 69 67 61 74 6f 72 2e 75 73 65 72 41 67 65 6e 74 2e 69 6e 64 65 78 4f 66 28 22 54 72 69 64 65 6e 74 22 29 21 3d 3d 2d 31 29 7b 76 61 72 20 69 65 42 61 6e 6e 65 72 44 69 76 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 49 45 2d 77 61 72 6e 69 6e 67 22 29 3b 69 66 28 69 65 42 61 6e 6e 65 72 44 69 76 29 7b 69 65 42 61 6e 6e 65 72 44 69 76 2e 63 6c 61 73 73 4c 69 73 74 2e 72 65 6d 6f 76 65 28 22 49 45 2d 77 61 72 6e 69 6e 67 2d 68 69 64 65 22 29 7d 7d 7d 73 68 6f 77 49 45 42 61 6e 6e 65 72 28 29 Data Ascii: show_locales?fade_out:fade_in)("locale-footer"))}function showIEBanner(){if(navigator.userAgent.indexOf("Trident")!==-1){var ieBannerDiv=document.getElementById("IE-warning");if(ieBannerDiv){ieBannerDiv.classList.remove("IE-warning-hide")}}}showIEBanner()
2022-05-27 05:41:35 UTC	829	IN	Data Raw: 68 69 73 2e 5f 75 72 6c 2b 22 3f 22 2b 70 61 73 73 44 61 74 61 2b 22 26 74 69 6d 65 73 74 61 6d 70 3d 22 2b 28 6e 65 77 20 44 61 74 65 29 2e 67 65 74 54 69 6d 65 28 29 3b 61 6a 61 78 2e 6f 70 65 6e 28 22 47 45 54 22 2c 75 72 69 2c 74 72 75 65 29 3b 61 6a 61 78 2e 73 65 6e 64 28 6e 75 6c 6c 29 7d 74 68 69 73 2e 41 4a 41 58 3d 61 6a 61 78 3b 74 68 69 73 2e 75 70 64 61 74 69 6e 67 3d 74 72 75 65 7d 63 61 74 63 68 28 65 29 7b 6c 6f 67 69 6e 5f 66 6f 72 6d 2e 73 75 62 6d 69 74 28 29 7d 72 65 74 75 72 6e 20 74 72 75 65 7d 3b 76 61 72 20 5f 74 65 78 74 5f 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 43 6f 6e 74 65 6e 74 22 69 6e 20 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 3f 22 74 65 78 74 43 6f 6e 74 65 6e 74 22 3a 22 69 6e 6e 65 72 54 65 78 74 22 3b 66 75 6e 63 74 69 Data Ascii: his._url+"?"+passData+"&timestamp="+(new Date).getTime();ajax.open("GET",uri,true);ajax.send(null)}this.AJAX=ajax;this.updating=true}catch(e){login_form.submit()}return true};var _text_content="textContent"in document.body?"textContent":"innerText";functi
2022-05-27 05:41:35 UTC	837	IN	Data Raw: 32 30 31 31 2c 32 2c 32 37 2c 31 2c 30 2c 30 2c 30 29 2c 22 45 75 72 6f 70 65 2f 48 65 6c 73 69 6e 6b 69 22 3a 6e 65 77 20 44 61 74 65 28 32 30 31 31 2c 32 2c 32 37 2c 34 2c 30 2c 30 2c 30 29 2c 22 45 75 72 6f 70 65 2f 49 73 74 61 6e 62 75 6c 22 3a 6e 65 77 20 44 61 74 65 28 32 30 31 31 2c 32 2c 32 38 2c 35 2c 30 2c 30 2c 30 29 2c 22 41 73 69 61 2f 44 61 6d 61 73 63 75 73 22 3a 6e 65 77 20 44 61 74 65 28 32 30 31 31 2c 33 2c 31 2c 32 2c 30 2c 30 2c 30 29 2c 22 41 73 69 61 2f 4a 65 72 75 73 61 6c 65 6d 22 3a 6e 65 77 20 44 61 74 65 28 32 30 31 31 2c 33 2c 31 2c 36 2c 30 2c 30 2c 30 29 2c 22 41 73 69 61 2f 47 61 7a 61 22 3a 6e 65 77 20 44 61 74 65 28 32 30 30 39 2c 32 2c 32 38 2c 30 2c 33 30 2c 30 2c 30 29 2c 22 41 66 72 69 63 61 2f 43 61 69 72 6f 22 3a 6e Data Ascii: 2011,2,27,1,0,0,0),"Europe/Helsinki":new Date(2011,2,27,4,0,0,0),"Europe/Istanbul":new Date(2011,2,28,5,0,0,0),"Asia/Damascus":new Date(2011,3,1,2,0,0,0),"Asia/Jerusalem":new Date(2011,3,1,6,0,0,0),"Asia/Gaza":new Date(2009,2,28,0,30,0,0),"Africa/Cairo":n
2022-05-27 05:41:35 UTC	842	IN	Data Raw: 29 7b 76 61 72 20 64 65 74 65 63 74 65 64 5f 6e 6f 64 65 73 3d 64 6f 63 75 6d 65 6e 74 2e 71 75 65 72 79 53 65 6c 65 63 74 6f 72 41 6c 6c 28 22 2e 22 2b 44 45 54 45 43 54 45 44 5f 54 5a 5f 43 4c 41 53 53 29 3b 5b 5d 2e 66 6f 72 45 61 63 68 2e 63 61 6c 6c 28 64 65 74 65 63 74 65 64 5f 6e 6f 64 65 73 2c 28 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 6e 2e 74 65 78 74 43 6f 6e 74 65 6e 74 3d 64 65 74 65 63 74 65 64 5f 74 7a 7d 29 29 3b 76 61 72 20 73 68 6f 77 5f 6e 6f 64 65 73 3d 64 6f 63 75 6d 65 6e 74 2e 71 75 65 72 79 53 65 6c 65 63 74 6f 72 41 6c 6c 28 22 2e 22 2b 43 4f 4f 4b 49 45 5f 54 49 4d 45 5a 4f 4e 45 5f 4d 49 53 4d 41 54 43 48 5f 43 4c 41 53 53 29 3b 5b 5d 2e 66 6f 72 45 61 63 68 2e 63 61 6c 6c 28 73 68 6f 77 5f 6e 6f 64 65 73 2c 28 66 75 6e 63 74 69 6f Data Ascii:){var detected_nodes=document.querySelectorAll("."+DETECTED_TZ_CLASS);[].forEach.call(detected_nodes,(function(n){n.textContent=detected_tz}));var show_nodes=document.querySelectorAll("."+COOKIE_TIMEZONE_MISMATCH_CLASS);[].forEach.call(show_nodes,(functio

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49966	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:37 UTC	843	OUT	GET /?locale=es HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: roundcube_cookies=enabled; timezone=America/Los_Angeles; webmailsession=%3atv2V2gFhVsVxQnAL%2ca29dc2d32ccadd90323922aa2d946414; session_locale=el
2022-05-27 05:41:37 UTC	843	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:37 GMT Server: Apache Content-Type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 38348 Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: webmailsession=%3arwNXY9Q5iIf01mfQ%2cb3126fa745e92fde4aa60bc70961e113; HttpOnly; path=/; port=443; secure Set-Cookie: session_locale=es; expires=Sat, 27-May-2023 05:41:37 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=443; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: imp_key=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 27-May-2023 05:41:37 GMT; path=/; port=443; secure Connection: close
2022-05-27 05:41:37 UTC	845	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 73 22 20 64 69 72 3d 22 6c 74 72 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f Data Ascii: <!DOCTYPE html><html lang="es" dir="ltr"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1"> <meta name="goo
2022-05-27 05:41:37 UTC	851	IN	Data Raw: 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 6d 65 73 73 61 67 65 22 3e 54 68 65 20 73 79 73 74 65 6d 20 68 61 73 20 64 65 74 65 63 74 65 64 20 74 68 61 74 20 79 6f 75 20 61 72 65 20 75 73 69 6e 67 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 63 50 61 6e 65 6c 20 26 61 6d 70 3b 20 57 48 4d 20 6e 6f 20 6c 6f 6e 67 65 72 20 73 75 70 70 6f 72 74 73 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 72 65 61 64 20 74 68 65 20 3c 61 20 74 69 74 6c 65 3d 22 63 50 61 6e 65 6c 20 42 6c 6f 67 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6f 2e 63 70 61 6e 65 6c 2e 6e 65 74 2f 69 Data Ascii: <div id="IE-warning-message">The system has detected that you are using Internet Explorer 11. cPanel & WHM no longer supports Internet Explorer 11. For more information, read the <a title="cPanel Blog" target="_blank" href="https://go.cpanel.net/i
2022-05-27 05:41:37 UTC	853	IN	Data Raw: 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 22 3e 73 75 6f 6d 69 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 6c 22 3e 46 69 6c 69 70 69 6e 6f 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 Data Ascii: <div class="locale-cell">suomi</div> <div class="locale-cell">Filipino</div>
2022-05-27 05:41:37 UTC	861	IN	Data Raw: c3 bc 72 6b c3 a7 65 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 75 6b 27 3e d1 83 d0 ba d1 80 d0 b0 d1 97 d0 bd d1 81 d1 8c d0 ba d0 b0 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 76 69 27 3e 54 69 e1 ba bf 6e 67 20 56 69 e1 bb 87 74 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 27 3e e4 b8 ad e6 96 87 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 5f 63 6e 27 3e e4 b8 ad e6 96 87 ef bc 88 e4 b8 ad e5 9b bd ef bc 89 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 5f 74 77 27 3e e4 b8 ad e6 96 87 ef bc 88 e5 8f b0 e6 b9 be ef bc 89 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 65 73 Data Ascii: rke</option><option value='uk'></option><option value='vi'>Ting Vit</option><option value='zh'></option><option value='zh_cn'></option><option value='zh_tw'></option><option value='es

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:37 UTC	867	IN	Data Raw: 69 64 64 65 6e 22 29 7b 69 66 28 77 69 6e 64 6f 77 2e 67 65 74 43 6f 6d 70 75 74 65 64 53 74 79 6c 65 29 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 4e 75 6d 62 65 72 28 63 75 72 5f 73 74 79 6c 65 2e 6f 70 61 63 69 74 79 29 7d 65 6c 73 65 7b 74 72 79 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 65 6c 2e 66 69 6c 74 65 72 73 2e 69 74 65 6d 28 22 44 58 49 6d 61 67 65 54 72 61 6e 73 66 6f 72 6d 2e 4d 69 63 72 6f 73 6f 66 74 2e 41 6c 70 68 61 22 29 2e 6f 70 61 63 69 74 79 7d 63 61 74 63 68 28 65 29 7b 74 72 79 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 65 6c 2e 66 69 6c 74 65 72 73 28 22 61 6c 70 68 61 22 29 2e 6f 70 61 63 69 74 79 7d 63 61 74 63 68 28 65 72 72 6f 72 29 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 31 30 30 7d 7d 73 74 61 72 74 5f 6f 70 61 Data Ascii: idden"){if(window.getComputedStyle){start_opacity=Number(cur_style.opacity)}else{try{start_opacity=el.filters.item("DXImageTransform.Microsoft.Alpha").opacity}catch(e){try{start_opacity=el.filters("alpha").opacity}catch(error){start_opacity=100}}start_opa
2022-05-27 05:41:37 UTC	869	IN	Data Raw: 74 69 6f 6e 5f 6f 62 6a 5f 74 6f 5f 72 65 64 69 72 65 63 74 3d 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 7d 65 6c 73 65 7b 69 66 28 72 65 73 75 6c 74 2e 73 65 63 75 72 69 74 79 5f 74 6f 6b 65 6e 26 26 74 6f 70 21 3d 3d 77 69 6e 64 6f 77 29 7b 66 6f 72 28 76 61 72 20 66 3d 30 3b 66 3c 74 6f 70 2e 66 72 61 6d 65 73 2e 6c 65 6e 67 74 68 3b 66 2b 2b 29 7b 69 66 28 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 21 3d 3d 77 69 6e 64 6f 77 29 7b 76 61 72 20 68 72 65 66 3d 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 2e 72 65 70 6c 61 63 65 28 2f 5c 2f 63 70 73 65 73 73 5b 2e 5c 64 5d 2b 2f 2c 72 65 73 75 6c 74 2e 73 65 63 75 72 69 74 79 5f 74 6f 6b 65 6e 29 3b 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 Data Ascii: tion_obj_to_redirect=top.location}else{if(result.security_token&&top!==window){for(var f=0;f<top.frames.length;f++){if(top.frames[f]!==window){var href=top.frames[f].location.href.replace(/\/cpsess[.\d]+/,result.security_token);top.frames[f].location.href
2022-05-27 05:41:37 UTC	877	IN	Data Raw: 28 32 30 31 31 2c 32 2c 32 37 2c 31 2c 30 2c 30 2c 30 29 2c 22 45 75 72 6f 70 65 2f 4d 6f 73 63 6f 77 22 3a 74 2c 22 41 73 69 61 2f 59 65 6b 61 74 65 72 69 6e 62 75 72 67 22 3a 74 2c 22 41 73 69 61 2f 4f 6d 73 6b 22 3a 74 2c 22 41 73 69 61 2f 4b 72 61 73 6e 6f 79 61 72 73 6b 22 3a 74 2c 22 41 73 69 61 2f 49 72 6b 75 74 73 6b 22 3a 74 2c 22 41 73 69 61 2f 59 61 6b 75 74 73 6b 22 3a 74 2c 22 41 73 69 61 2f 56 6c 61 64 69 76 6f 73 74 6f 6b 22 3a 74 2c 22 41 73 69 61 2f 4b 61 6d 63 68 61 74 6b 61 22 3a 74 2c 22 45 75 72 6f 70 65 2f 4d 69 6e 73 6b 22 3a 74 2c 22 41 75 73 74 72 61 6c 69 61 2f 50 65 72 74 68 22 3a 6e 65 77 20 44 61 74 65 28 32 30 30 38 2c 31 30 2c 31 2c 31 2c 30 2c 30 2c 30 29 7d 3b 72 65 74 75 72 6e 20 6e 5b 65 5d 7d 3b 72 65 74 75 72 6e 7b 64 Data Ascii: (2011,2,27,1,0,0,0),"Europe/Moscow":t,"Asia/Yekaterinburg":t,"Asia/Omsk":t,"Asia/Krasnoyarsk":t,"Asia/Irkutsk":t,"Asia/Yakutsk":t,"Asia/Vladivostok":t,"Asia/Kamchatka":t,"Europe/Minsk":t,"Australia/Perth":new Date(2008,10,1,1,0,0,0)};return n[e]};return{d
2022-05-27 05:41:37 UTC	883	IN	Data Raw: 3b 0a 0a 0a 43 50 54 69 6d 65 7a 6f 6e 65 2e 72 65 73 65 74 5f 74 69 6d 65 7a 6f 6e 65 28 29 3b 0a 3c 2f 73 63 72 69 70 74 3e 0a 0a 3c 73 74 79 6c 65 3e 0a 20 20 20 20 40 6d 65 64 69 61 20 28 6d 69 6e 2d 77 69 64 74 68 3a 20 34 38 31 70 78 29 20 7b 0a 20 20 20 20 20 20 20 20 23 73 65 6c 65 63 74 5f 75 73 65 72 5f 66 6f 72 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 70 78 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 70 79 72 69 67 68 74 22 3e 43 6f 70 79 72 69 67 68 74 c2 a9 c2 a0 32 30 32 32 20 63 50 61 6e 65 6c 2c 20 4c 2e 4c 2e 43 2e 0a 20 20 20 20 3c 62 72 20 2f 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6f 2e 63 70 61 6e 65 Data Ascii: ;CPTimezone.reset_timezone();</script><style> @media (min-width: 481px) { #select_user_form { width: px; } }</style> Copyright2022 cPanel, L.L.C. <a href="https://go.cpane

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49975	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:47 UTC	883	OUT	GET /?locale=ar HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: roundcube_cookies=enabled; timezone=America/Los_Angeles; webmailsession=%3arwNXY9Q5ilf01mfQ%2cb3126fa745e92fde4aa60bc70961e113; session_locale=es

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:47 UTC	884	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:47 GMT Server: Apache Content-Type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 38811 Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: webmailsession=%3a6uJKuDYKo5yL312X%2c723f4495b1a66df427ab5eca1e9f6fce; HttpOnly; path=/; port=443; secure Set-Cookie: session_locale=ar; expires=Sat, 27-May-2023 05:41:47 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=443; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: imp_key=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 27-May-2023 05:41:47 GMT; path=/; port=443; secure Connection: close
2022-05-27 05:41:47 UTC	885	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 61 72 22 20 64 69 72 3d 22 72 74 6c 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f Data Ascii: <!DOCTYPE html><html lang="ar" dir="rtl"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1"> <meta name="goo
2022-05-27 05:41:47 UTC	892	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 69 63 6f 6e 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 69 63 6f 6e 22 3e 3c 2f 73 70 61 6e 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 6d 65 73 73 61 67 65 22 3e 54 68 65 20 73 79 73 74 65 6d 20 68 61 73 20 64 65 74 65 63 74 65 64 20 74 68 61 74 20 79 6f 75 20 61 72 65 20 75 73 69 6e 67 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 63 50 61 6e 65 6c 20 26 61 6d 70 3b 20 57 48 4d 20 6e 6f 20 6c 6f 6e 67 65 72 20 73 75 70 70 6f 72 74 73 20 49 6e 74 65 72 6e 65 74 20 45 78 Data Ascii: <div id="IE-warning-icon-container"></div> <div id="IE-warning-message">The system has detected that you are using Internet Explorer 11. cPanel & WHM no longer supports Internet Ex
2022-05-27 05:41:47 UTC	893	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 65 73 5f 65 73 22 3e 65 73 70 61 c3 b1 6f 6c 20 64 65 20 45 73 70 61 c3 b1 61 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 22 3e 73 75 6f 6d 69 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 Data Ascii: <div class="locale-cell">espaol de Espaa</div> <div class="locale-cell">suomi</div>
2022-05-27 05:41:47 UTC	901	IN	Data Raw: 73 69 6c 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 72 6f 27 3e 72 6f 6d c3 a2 6e c4 83 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 72 75 27 3e d1 80 d1 83 d1 81 d1 81 d0 ba d0 b8 d0 b9 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 73 6c 27 3e 73 6c 6f 76 65 6e c5 a1 c4 8d 69 6e 61 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 73 76 27 3e 73 76 65 6e 73 6b 61 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 74 68 27 3e e0 b9 84 e0 b8 97 e0 b8 a2 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 74 72 27 3e 54 c3 bc 72 6b c3 a7 65 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 75 Data Ascii: sil</option><option value='ro'>romn</option><option value='ru'></option><option value='sl'>slovenina</option><option value='sv'>svenska</option><option value='th'></option><option value='tr'>Trke</option><option value='u
2022-05-27 05:41:47 UTC	907	IN	Data Raw: 69 67 61 74 6f 72 2e 75 73 65 72 41 67 65 6e 74 2e 69 6e 64 65 78 4f 66 28 22 54 72 69 64 65 6e 74 22 29 21 3d 3d 2d 31 29 7b 76 61 72 20 69 65 42 61 6e 6e 65 72 44 69 76 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 49 45 2d 77 61 72 6e 69 6e 67 22 29 3b 69 66 28 69 65 42 61 6e 6e 65 72 44 69 76 29 7b 69 65 42 61 6e 6e 65 72 44 69 76 2e 63 6c 61 73 73 4c 69 73 74 2e 72 65 6d 6f 76 65 28 22 49 45 2d 77 61 72 6e 69 6e 67 2d 68 69 64 65 22 29 7d 7d 7d 73 68 6f 77 49 45 42 61 6e 6e 65 72 28 29 3b 66 75 6e 63 74 69 6f 6e 20 66 61 64 65 5f 69 6e 28 65 6c 2c 64 75 72 61 74 69 6f 6e 2c 5f 66 61 64 65 5f 6f 75 74 5f 69 6e 73 74 65 61 64 29 7b 65 6c 3d 64 69 76 5f 63 61 63 68 65 5b 65 6c 5d 7c 7c 44 4f 4d 2e 67 65 74 28 65 6c 29 7c Data Ascii: igator.userAgent.indexOf("Trident")!==-1){var ieBannerDiv=document.getElementById("IE-warning");if(ieBannerDiv){ieBannerDiv.classList.remove("IE-warning-hide")}}}showIEBanner();function fade_in(el,duration,_fade_out_instead){el=div_cache[el]||DOM.get(el)|

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:47 UTC	909	IN	Data Raw: 75 65 29 3b 61 6a 61 78 2e 73 65 6e 64 28 6e 75 6c 6c 29 7d 74 68 69 73 2e 41 4a 41 58 3d 61 6a 61 78 3b 74 68 69 73 2e 75 70 64 61 74 69 6e 67 3d 74 72 75 65 7d 63 61 74 63 68 28 65 29 7b 6c 6f 67 69 6e 5f 66 6f 72 6d 2e 73 75 62 6d 69 74 28 29 7d 72 65 74 75 72 6e 20 74 72 75 65 7d 3b 76 61 72 20 5f 74 65 78 74 5f 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 43 6f 6e 74 65 6e 74 22 69 6e 20 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 3f 22 74 65 78 74 43 6f 6e 74 65 6e 74 22 3a 22 69 6e 6e 65 72 54 65 78 74 22 3b 66 75 6e 63 74 69 6f 6e 20 5f 70 72 6f 63 65 73 73 5f 70 61 72 73 65 64 5f 6c 6f 67 69 6e 5f 73 75 63 63 65 73 73 28 72 65 73 75 6c 74 29 7b 76 61 72 20 66 69 6e 61 6c 5f 75 72 69 3b 76 61 72 20 6c 6f 67 69 6e 5f 75 72 6c 5f 72 65 67 65 78 3d 2f 5e 5c 2f Data Ascii: ue);ajax.send(null)}this.AJAX=ajax;this.updating=true}catch(e){login_form.submit()}return true};var _text_content="textContent"in document.body?"textContent":"innerText";function _process_parsed_login_success(result){var final_uri;var login_url_regex=/^\/
2022-05-27 05:41:47 UTC	917	IN	Data Raw: 75 6c 22 3a 6e 65 77 20 44 61 74 65 28 32 30 31 31 2c 32 2c 32 38 2c 35 2c 30 2c 30 2c 30 29 2c 22 41 73 69 61 2f 44 61 6d 61 73 63 75 73 22 3a 6e 65 77 20 44 61 74 65 28 32 30 31 31 2c 33 2c 31 2c 32 2c 30 2c 30 2c 30 29 2c 22 41 73 69 61 2f 4a 65 72 75 73 61 6c 65 6d 22 3a 6e 65 77 20 44 61 74 65 28 32 30 31 31 2c 33 2c 31 2c 36 2c 30 2c 30 2c 30 29 2c 22 41 73 69 61 2f 47 61 7a 61 22 3a 6e 65 77 20 44 61 74 65 28 32 30 30 39 2c 32 2c 32 38 2c 30 2c 33 30 2c 30 2c 30 29 2c 22 41 66 72 69 63 61 2f 43 61 69 72 6f 22 3a 6e 65 77 20 44 61 74 65 28 32 30 30 39 2c 33 2c 32 35 2c 30 2c 33 30 2c 30 2c 30 29 2c 22 50 61 63 69 66 69 63 2f 41 75 63 6b 6c 61 6e 64 22 3a 6e 65 77 20 44 61 74 65 28 32 30 31 31 2c 38 2c 32 36 2c 37 2c 30 2c 30 2c 30 29 2c 22 50 61 63 Data Ascii: ul":new Date(2011,2,28,5,0,0,0),"Asia/Damascus":new Date(2011,3,1,2,0,0,0),"Asia/Jerusalem":new Date(2011,3,1,6,0,0,0),"Asia/Gaza":new Date(2009,2,28,0,30,0,0),"Africa/Cairo":new Date(2009,3,25,0,30,0,0),"Pacific/Auckland":new Date(2011,8,26,7,0,0,0),"Pac
2022-05-27 05:41:47 UTC	923	IN	Data Raw: 68 2e 63 61 6c 6c 28 64 65 74 65 63 74 65 64 5f 6e 6f 64 65 73 2c 28 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 6e 2e 74 65 78 74 43 6f 6e 74 65 6e 74 3d 64 65 74 65 63 74 65 64 5f 74 7a 7d 29 29 3b 76 61 72 20 73 68 6f 77 5f 6e 6f 64 65 73 3d 64 6f 63 75 6d 65 6e 74 2e 71 75 65 72 79 53 65 6c 65 63 74 6f 72 41 6c 6c 28 22 2e 22 2b 43 4f 4f 4b 49 45 5f 54 49 4d 45 5a 4f 4e 45 5f 4d 49 53 4d 41 54 43 48 5f 43 4c 41 53 53 29 3b 5b 5d 2e 66 6f 72 45 61 63 68 2e 63 61 6c 6c 28 73 68 6f 77 5f 6e 6f 64 65 73 2c 28 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 6e 2e 63 6c 61 73 73 4e 61 6d 65 2b 3d 22 20 22 2b 53 48 4f 57 4e 5f 43 4c 41 53 53 7d 29 29 7d 7d 77 69 6e 64 6f 77 2e 43 50 54 69 6d 65 7a 6f 6e 65 3d 7b 73 68 6f 77 5f 63 6f 6f 6b 69 65 5f 74 69 6d 65 7a 6f 6e 65 5f 6d Data Ascii: h.call(detected_nodes,(function(n){n.textContent=detected_tz}));var show_nodes=document.querySelectorAll("."+COOKIE_TIMEZONE_MISMATCH_CLASS);[].forEach.call(show_nodes,(function(n){n.className+=" "+SHOWN_CLASS}))}}window.CPTimezone={show_cookie_timezone_m

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	50003	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:49 UTC	923	OUT	GET /?locale=bg HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: roundcube_cookies=enabled; timezone=America/Los_Angeles; webmailsession=%3a6uJKuDYKo5yL312X%2c723f4495b1a66df427ab5eca1e9f6fce; session_locale=ar

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:49 UTC	924	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:49 GMT Server: Apache Content-Type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 37802 Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: webmailsession=%3aV8tkTA7rl56zmE8l%2c7b0d62de45651f81f78e4d680c484c2d; HttpOnly; path=/; port=443; secure Set-Cookie: session_locale=bg; expires=Sat, 27-May-2023 05:41:49 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 0 0:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00 :00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=443; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: imp_key=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00 :00:01 GMT; path=/; port=443 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 27-May-2023 05:41:49 GMT; path=/; port=443; secure Connection: close
2022-05-27 05:41:49 UTC	926	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 62 67 22 20 64 69 72 3d 22 6c 74 72 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f Data Ascii: <!DOCTYPE html><html lang="bg" dir="ltr"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1"> <meta name="goo
2022-05-27 05:41:49 UTC	932	IN	Data Raw: 67 65 22 3e 54 68 65 20 73 79 73 74 65 6d 20 68 61 73 20 64 65 74 65 63 74 65 64 20 74 68 61 74 20 79 6f 75 20 61 72 65 20 75 73 69 6e 67 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 63 50 61 6e 65 6c 20 26 61 6d 70 3b 20 57 48 4d 20 6e 6f 20 6c 6f 6e 67 65 72 20 73 75 70 70 6f 72 74 73 20 49 6e 74 65 72 6e 65 74 2 0 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 72 65 61 64 2 0 74 68 65 20 3c 61 20 74 69 74 6c 65 3d 22 63 50 61 6e 65 6c 20 42 6c 6f 67 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6f 2e 63 70 61 6e 65 6c 2e 6e 65 74 2f 69 65 31 31 64 65 70 72 65 63 61 74 69 6f 6e 22 3e 63 50 61 6e 65 6c 20 42 6c 6f 67 3c 2f Data Ascii: ge">The system has detected that you are using Internet Explorer 11. cPanel & WHM no longer supports Internet Explorer 11. For more information, read the <a title="cPanel Blog" target="_blank" href="https://go.cpanel.net/ie1 1deprecation">cPanel Blog</
2022-05-27 05:41:49 UTC	934	IN	Data Raw: 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 22 3e 73 75 6f 6d 69 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 6c 22 3e 46 69 6c 69 70 69 6e 6f 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 6 5 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d Data Ascii: ll">suomi</div> <div class="locale-cell">Filipino</div> <div class="locale-cell"><a href="?locale=
2022-05-27 05:41:49 UTC	942	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 62 75 74 74 6f 6e 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 31 30 70 78 22 20 74 79 70 65 3d 22 73 75 62 6d 69 74 22 3e 43 68 61 6e 67 65 3c 2f 62 75 74 74 6f 6e 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 66 6f 72 6d 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 23 6d 6f 62 69 6c 65 6c 6f 63 61 6c 65 6d 65 6e 75 2c 20 23 6c 6f 63 61 6c 65 73 5f 6c 69 73 74 20 7b 64 69 73 70 6c 61 79 3a 6 e 6f 6e 65 7d 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 6e 6f 73 63 72 69 70 74 3 e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 75 6c 20 Data Ascii: <button style="margin-left: 10px" type="submit">Change</button> </form> <style type="text/css">#mobilelocalemenu, #locales_list {display:none}</style> </noscript> <ul
2022-05-27 05:41:49 UTC	947	IN	Data Raw: 61 74 69 6f 6e 5f 6d 73 2b 73 74 61 72 74 2e 67 65 74 54 69 6d 65 28 29 7d 65 6c 73 65 7b 73 74 79 6c 65 5f 6f 62 6a 2e 76 69 73 69 62 69 6c 69 74 79 3d 22 76 69 73 69 62 6c 65 22 7d 76 61 72 20 66 61 64 65 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 6f 70 61 63 69 74 79 3b 69 66 28 5f 66 61 64 65 5f 6f 75 74 5f 69 6e 73 74 65 61 64 29 7b 6f 70 61 63 69 74 79 3d 73 74 61 72 74 5f 6f 70 61 63 69 74 79 2a 28 65 6e 64 2d 6e 65 77 20 44 61 74 65 29 2f 64 75 72 61 74 69 6f 6e 5f 6d 73 3b 69 66 28 6f 70 61 63 69 74 79 3c 3d 30 29 7b 6f 70 61 63 69 74 79 3d 30 3b 63 6c 65 61 72 49 6e 74 65 72 76 61 6c 28 69 6e 74 65 72 76 61 6c 29 3b 73 74 79 6c 65 5f 6f 62 6a 2e 76 69 73 69 62 69 6c 69 74 79 3d 22 68 69 64 64 65 6e 22 7d 7d 65 6c 73 65 7b 6f 70 61 63 69 Data Ascii: ation_ms+start.getTime()}else{style_obj.visibility="visible"}var fader=function(){var opacity;if(_fade_out_i nstead){opacity=start_opacity*(end-new Date)/duration_ms;if(opacity<=0){opacity=0;clearInterval(interval);style_obj.visi bility="hidden"}}else{opaci

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:49 UTC	950	IN	Data Raw: 6f 74 69 63 65 73 22 29 3b 66 6f 72 28 76 61 72 20 6e 3d 30 3b 6e 3c 72 65 73 75 6c 74 2e 6e 6f 74 69 63 65 73 2e 6c 65 6e 67 74 68 3b 6e 2b 2b 29 7b 76 61 72 20 6e 65 77 5f 70 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 70 22 29 3b 6e 65 77 5f 70 2e 74 65 78 74 43 6f 6e 74 65 6e 74 3d 72 65 73 75 6c 74 2e 6e 6f 74 69 63 65 73 5b 6e 5d 2e 63 6f 6e 74 65 6e 74 3b 63 6f 6e 74 61 69 6e 65 72 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 6e 65 77 5f 70 29 7d 63 6c 69 63 6b 5f 66 6f 72 6d 2e 6f 6e 73 75 62 6d 69 74 3d 72 65 64 69 72 65 63 74 6f 72 3b 66 61 64 65 5f 6f 75 74 28 6c 6f 67 69 6e 5f 66 6f 72 6d 29 3b 66 61 64 65 5f 69 6e 28 63 6c 69 63 6b 5f 66 6f 72 6d 29 7d 65 6c 73 65 7b 73 68 6f 77 5f 73 74 61 74 75 73 28 4d 45 53 53 41 Data Ascii: otices");for(var n=0;n<result.notices.length;n++){var new_p=document.createElement("p");new_p.text Content=result.notices[n].content;container.appendChild(new_p)}click_form.onsubmit=redirector;fade_out(login_f orm);fade_in(click_form)}else{show_status(MESSA
2022-05-27 05:41:49 UTC	958	IN	Data Raw: 63 61 2f 4d 6f 6e 74 65 76 69 64 65 6f 22 3a 5b 22 41 6d 65 72 69 63 61 2f 4d 6f 6e 74 65 76 69 64 65 6f 22 2c 22 41 6d 65 72 69 63 61 2f 53 61 6f 5f 50 61 75 6c 6f 22 5d 2c 22 41 73 69 61 2f 42 65 69 72 75 74 22 3a 5b 22 41 73 69 61 2f 42 65 69 72 75 74 22 2c 22 45 75 72 6f 70 65 2f 48 65 6c 73 69 6e 6b 69 22 2c 22 45 75 72 6f 70 65 2f 49 73 74 61 6e 62 75 6c 22 2c 22 41 73 69 61 2f 44 61 6d 61 73 63 75 73 22 2c 22 41 73 69 61 2f 4a 65 72 75 73 61 6c 65 6d 22 2c 22 41 73 69 61 2f 47 61 7a 61 22 5d 2c 22 50 61 63 69 66 69 63 2f 41 75 63 6b 6c 61 6e 64 22 3a 5b 22 50 61 63 69 66 69 63 2f 41 75 63 6b 6c 61 6e 64 22 2c 22 50 61 63 69 66 69 63 2f 46 69 6a 69 22 5d 2c 22 41 6d 65 72 69 63 61 2f 4c 6f 73 5f 41 6e 67 65 6c 65 73 22 3a 5b 22 41 6d 65 72 69 63 61 Data Ascii: ca/Montevideo":["America/Montevideo","America/Sao_Paulo"],"Asia/Beirut":["Asia/Beirut","Europe/Helsinki","Eu rope/Istanbul","Asia/Damascus","Asia/Jerusalem","Asia/Gaza"],"Pacific/Auckland":["Pacific/Auckland","Pacific/Fiji"],"Ame rica/Los_Angeles":["America

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	50011	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:51 UTC	963	OUT	GET /?locale=cs HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183. 121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig ned-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: roundcube_cookies=enabled; timezone=America/Los_Angeles; webmailsession=%3aV8tkTA7rl56zmE8l% 2c7b0d62de45651f81f78e4d680c484c2d; session_locale=bg
2022-05-27 05:41:51 UTC	964	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:51 GMT Server: Apache Content-Type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 38244 Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: webmailsession=%3alcZ7fzgMFJwE7Gs3%2ce9b32721a3479df213bc57116d918206; HttpOnly; path=/; port=443; secure Set-Cookie: session_locale=cs; expires=Sat, 27-May-2023 05:41:51 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 0 0:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00 :00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=443; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: imp_key=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00 :00:01 GMT; path=/; port=443 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 27-May-2023 05:41:51 GMT; path=/; port=443; secure Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:51 UTC	966	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 63 73 22 20 64 69 72 3d 22 6c 74 72 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f Data Ascii: <!DOCTYPE html><html lang="cs" dir="ltr"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1"> <meta name="goo
2022-05-27 05:41:51 UTC	972	IN	Data Raw: 6c 61 73 73 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 69 63 6f 6e 22 3e 3c 2f 73 70 61 6e 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 6d 65 73 73 61 67 65 22 3e 54 68 65 20 73 79 73 74 65 6d 20 68 61 73 20 64 65 74 65 63 74 65 64 20 74 68 61 74 20 79 6f 75 20 61 72 65 20 75 73 69 6e 67 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 63 50 61 6e 65 6c 20 26 61 6d 70 3b 20 57 48 4d 20 6e 6f 20 6c 6f 6e 67 65 72 20 73 75 70 70 6f 72 74 73 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 72 65 61 64 20 74 68 65 20 3c 61 20 74 69 74 6c 65 3d 22 63 50 61 6e 65 Data Ascii: lass="IE-warning-icon"></div> <div id="IE-warning-message">The system has detected that you are using Internet Explorer 11. cPanel & WHM no longer supports Internet Explorer 11. For more information , read the <a title="cPane
2022-05-27 05:41:51 UTC	974	IN	Data Raw: 61 c3 b1 6f 6c 20 64 65 20 45 73 70 61 c3 b1 61 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 22 3e 73 75 6f 6d 69 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 6c 22 3e 46 69 6c 69 70 69 6e 6f 3c 2f 61 3e 3c Data Ascii: aol de Espaa</div> <div class="locale-cell">suomi</div> <div class="locale-cell">Filipino<
2022-05-27 05:41:51 UTC	982	IN	Data Raw: 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 75 6b 27 3e d1 83 d0 ba d1 80 d0 b0 d1 97 d0 bd d1 81 d1 8c d0 ba d0 b0 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 76 69 27 3e 54 69 e1 ba bf 6e 67 20 56 69 e1 bb 87 74 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 27 3e e4 b8 ad e6 96 87 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 5f 63 6e 27 3e e4 b8 ad e6 96 87 ef bc 88 e4 b8 ad e5 9b bd ef bc 89 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 5f 74 77 27 3e e4 b8 ad e6 96 87 ef bc 88 e5 8f b0 e6 b9 be ef bc 89 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 63 73 27 3e c4 8d 65 c5 a1 74 69 6e 61 3c 2f 6f Data Ascii: n><option value='uk'></option><option value='vi'>Ting Vit</option><option value='zh'></option><option value='zh_cn'></option><option value='zh_tw'></option><option value='cs'>etina</o
2022-05-27 05:41:51 UTC	987	IN	Data Raw: 6c 74 65 72 73 2e 69 74 65 6d 28 22 44 58 49 6d 61 67 65 54 72 61 6e 73 66 6f 72 6d 2e 4d 69 63 72 6f 73 6f 66 74 2e 41 6c 70 68 61 22 29 2e 6f 70 61 63 69 74 79 7d 63 61 74 63 68 28 65 29 7b 74 72 79 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 65 6c 2e 66 69 6c 74 65 72 73 28 22 61 6c 70 68 61 22 29 2e 6f 70 61 63 69 74 79 7d 63 61 74 63 68 28 65 72 72 6f 72 29 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 31 30 30 7d 7d 73 74 61 72 74 5f 6f 70 61 63 69 74 79 2f 3d 31 30 30 7d 69 66 28 21 73 74 61 72 74 5f 6f 70 61 63 69 74 79 29 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 30 7d 7d 65 6c 73 65 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 30 3b 73 65 74 5f 6f 70 61 63 69 74 79 28 65 6c 2c 30 29 7d 69 66 28 5f 66 61 64 65 5f 6f 75 74 5f 69 6e 73 74 65 61 Data Ascii: lters.item("DXImageTransform.Microsoft.Alpha").opacity}catch(e){try{start_opacity=el.filters("alpha").opacity}catch(error){start_opacity=100}}start_opacity/=100}if(!start_opacity){start_opacity=0}}else{start_opacity=0;set_opacity(el,0)}if(_fade_out_instea
2022-05-27 05:41:51 UTC	990	IN	Data Raw: 6c 65 6e 67 74 68 3b 66 2b 2b 29 7b 69 66 28 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 21 3d 3d 77 69 6e 64 6f 77 29 7b 76 61 72 20 68 72 65 66 3d 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 2e 72 65 70 6c 61 63 65 28 2f 5c 2f 63 70 73 65 73 73 5b 2e 5c 64 5d 2b 2f 2c 72 65 73 75 6c 74 2e 73 65 63 75 72 69 74 79 5f 74 6f 6b 65 6e 29 3b 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 68 72 65 66 7d 7d 7d 6c 6f 63 61 74 69 6f 6e 5f 6f 62 6a 5f 74 6f 5f 72 65 64 69 72 65 63 74 3d 6c 6f 63 61 74 69 6f 6e 7d 76 61 72 20 72 65 64 69 72 65 63 74 6f 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 6c 6f 63 61 74 69 6f 6e 5f 6f 62 6a 5f 74 6f 5f 72 65 64 69 72 65 63 74 2e 68 72 65 66 3d 66 69 6e 61 6c 5f Data Ascii: length;f++){if(top.frames[f]!==window){var href=top.frames[f].location.href.replace(/\/cpsess[.\d]+/,result.security_token);top.frames[f].location.href=href}}}location_obj_to_redirect=location}var redirector=function(){location_obj_to_redirect.href=final_
2022-05-27 05:41:51 UTC	998	IN	Data Raw: 6b 75 74 73 6b 22 3a 74 2c 22 41 73 69 61 2f 59 61 6b 75 74 73 6b 22 3a 74 2c 22 41 73 69 61 2f 56 6c 61 64 69 76 6f 73 74 6f 6b 22 3a 74 2c 22 41 73 69 61 2f 4b 61 6d 63 68 61 74 6b 61 22 3a 74 2c 22 45 75 72 6f 70 65 2f 4d 69 6e 73 6b 22 3a 74 2c 22 41 75 73 74 72 61 6c 69 61 2f 50 65 72 74 68 22 3a 6e 65 77 20 44 61 74 65 28 32 30 30 38 2c 31 30 2c 31 2c 31 2c 30 2c 30 2c 30 29 7d 3b 72 65 74 75 72 6e 20 6e 5b 65 5d 7d 3b 72 65 74 75 72 6e 7b 64 65 74 65 72 6d 69 6e 65 3a 61 2c 64 61 74 65 5f 69 73 5f 64 73 74 3a 6f 2c 64 73 74 5f 73 74 61 72 74 5f 66 6f 72 3a 66 7d 7d 28 29 3b 74 2e 54 69 6d 65 5a 6f 6e 65 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 6e 3d 7b 22 41 6d 65 72 69 63 61 2f 44 65 6e 76 65 72 22 Data Ascii: kutsk":t,"Asia/Yakutsk":t,"Asia/Vladivostok":t,"Asia/Kamchatka":t,"Europe/Minsk":t,"Australia/Perth":new Date(2008,10,1,1,0,0,0)};return n[e]};return{determine:a,date_is_dst:o,dst_start_for:f}}();t.TimeZone=function(e){"use strict";var n={"America/Denver"
2022-05-27 05:41:51 UTC	1003	IN	Data Raw: 5f 66 6f 72 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 70 78 3b 0a 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 70 79 72 69 67 68 74 22 3e 43 6f 70 79 72 69 67 68 74 c2 a9 c2 a0 32 30 32 32 20 63 50 61 6e 65 6c 2c 20 4c 2e 4c 2e 43 2e 0a 20 20 20 20 3c 62 72 20 2f 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6f 2e 63 70 61 6e 65 6c 2e 6e 65 74 2f 70 72 69 76 61 63 79 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 3e 50 72 69 76 61 63 79 20 50 6f 6c 69 63 79 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 0a 3c 2f 62 6f 64 79 3e 0a 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: _form { width: px; } }</style> <div class="copyright">Copyright2022 cPanel, L.L.C. Privacy Policy</div></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	50019	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:53 UTC	1003	OUT	GET /?locale=da HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: roundcube_cookies=enabled; timezone=America/Los_Angeles; webmailsession=%3alcZ7fzgMFJwE7Gs3%2ce9b32721a3479df213bc57116d918206; session_locale=cs
2022-05-27 05:41:53 UTC	1004	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:53 GMT Server: Apache Content-Type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 38028 Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: webmailsession=%3aNtsC7AoBd2Q4g_iG%2cbb3e3b737d48efa9ace5acfe9a7f69ad; HttpOnly; path=/; port=443; secure Set-Cookie: session_locale=da; expires=Sat, 27-May-2023 05:41:53 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=443; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: imp_key=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 27-May-2023 05:41:53 GMT; path=/; port=443; secure Connection: close
2022-05-27 05:41:53 UTC	1005	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 64 61 22 20 64 69 72 3d 22 6c 74 72 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f Data Ascii: <!DOCTYPE html><html lang="da" dir="ltr"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1"> <meta name="goo
2022-05-27 05:41:53 UTC	1012	IN	Data Raw: 61 67 65 22 3e 54 68 65 20 73 79 73 74 65 6d 20 68 61 73 20 64 65 74 65 63 74 65 64 20 74 68 61 74 20 79 6f 75 20 61 72 65 20 75 73 69 6e 67 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 63 50 61 6e 65 6c 20 26 61 6d 70 3b 20 57 48 4d 20 6e 6f 20 6c 6f 6e 67 65 72 20 73 75 70 70 6f 72 74 73 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 72 65 61 64 20 74 68 65 20 3c 61 20 74 69 74 6c 65 3d 22 63 50 61 6e 65 6c 20 42 6c 6f 67 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6f 2e 63 70 61 6e 65 6c 2e 6e 65 74 2f 69 65 31 31 64 65 70 72 65 63 61 74 69 6f 6e 22 3e 63 50 61 6e 65 6c 20 42 6c 6f 67 3c Data Ascii: age">The system has detected that you are using Internet Explorer 11. cPanel & WHM no longer supports Internet Explorer 11. For more information, read the <a title="cPanel Blog" target="_blank" href="https://go.cpanel.net/ie11deprecation">cPanel Blog<
2022-05-27 05:41:53 UTC	1013	IN	Data Raw: 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 22 3e 73 75 6f 6d 69 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 6c 22 3e 46 69 6c 69 70 69 6e 6f 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 Data Ascii: s="locale-cell">suomi</div> <div class="locale-cell">Filipino</div> <div class="locale-cell"><a hr
2022-05-27 05:41:53 UTC	1021	IN	Data Raw: 68 27 3e e4 b8 ad e6 96 87 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 5f 63 6e 27 3e e4 b8 ad e6 96 87 ef bc 88 e4 b8 ad e5 9b bd ef bc 89 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 5f 74 77 27 3e e4 b8 ad e6 96 87 ef bc 88 e5 8f b0 e6 b9 be ef bc 89 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 64 61 27 3e 64 61 6e 73 6b 3c 2f 6f 70 74 69 6f 6e 3e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 73 65 6c 65 63 74 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 62 75 74 74 6f 6e 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 31 30 70 78 22 20 74 79 70 65 3d 22 73 75 62 6d 69 74 22 3e Data Ascii: h'></option><option value='zh_cn'></option><option value='zh_tw'></option><option value='da'>dansk</option> </select> <button style="margin-left: 10px" type="submit">

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:53 UTC	1027	IN	Data Raw: 30 3b 73 65 74 5f 6f 70 61 63 69 74 79 28 65 6c 2c 30 29 7d 69 66 28 5f 66 61 64 65 5f 6f 75 74 5f 69 6e 73 74 65 61 64 26 26 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3c 2e 30 31 29 7b 69 66 28 73 74 61 72 74 5f 6f 70 61 63 69 74 79 29 7b 73 65 74 5f 6f 70 61 63 69 74 79 28 65 6c 2c 30 29 7d 72 65 74 75 72 6e 7d 69 66 28 21 64 75 72 61 74 69 6f 6e 29 7b 64 75 72 61 74 69 6f 6e 3d 46 41 44 45 5f 44 55 52 41 54 49 4f 4e 7d 76 61 72 20 64 75 72 61 74 69 6f 6e 5f 6d 73 3d 64 75 72 61 74 69 6f 6e 2a 31 65 33 3b 76 61 72 20 73 74 61 72 74 3d 6e 65 77 20 44 61 74 65 3b 76 61 72 20 65 6e 64 3b 69 66 28 5f 66 61 64 65 5f 6f 75 74 5f 69 6e 73 74 65 61 64 29 7b 65 6e 64 3d 64 75 72 61 74 69 6f 6e 5f 6d 73 2b 73 74 61 72 74 2e 67 65 74 54 69 6d 65 28 29 7d 65 6c 73 65 Data Ascii: 0;set_opacity(el,0)}if(_fade_out_instead&&start_opacity<.01){if(start_opacity){set_opacity(el,0)}return}if(!duration){duration=FADE_DURATION}var duration_ms=duration*1e3;var start=new Date;var end;if(_fade_out_instead){end=duration_ms+start.getTime()}else
2022-05-27 05:41:53 UTC	1029	IN	Data Raw: 28 29 7b 6c 6f 63 61 74 69 6f 6e 5f 6f 62 6a 5f 74 6f 5f 72 65 64 69 72 65 63 74 2e 68 72 65 66 3d 66 69 6e 61 6c 5f 75 72 69 2b 6c 6f 63 61 74 69 6f 6e 2e 68 61 73 68 7d 3b 69 66 28 72 65 73 75 6c 74 2e 6e 6f 74 69 63 65 73 26 26 72 65 73 75 6c 74 2e 6e 6f 74 69 63 65 73 2e 6c 65 6e 67 74 68 29 7b 73 68 6f 77 5f 73 74 61 74 75 73 28 4d 45 53 53 41 47 45 53 2e 72 65 61 64 5f 62 65 6c 6f 77 2c 22 77 61 72 6e 22 29 3b 76 61 72 20 63 6c 69 63 6b 5f 66 6f 72 6d 3d 44 4f 4d 2e 67 65 74 28 22 63 6c 69 63 6b 74 68 72 6f 75 67 68 5f 66 6f 72 6d 22 29 3b 76 61 72 20 63 6f 6e 74 61 69 6e 65 72 3d 63 6c 69 63 6b 5f 66 6f 72 6d 2e 71 75 65 72 79 53 65 6c 65 63 74 6f 72 28 22 2e 6e 6f 74 69 63 65 73 22 29 3b 66 6f 72 28 76 61 72 20 6e 3d 30 3b 6e 3c 72 65 73 75 6c 74 Data Ascii: (){location_obj_to_redirect.href=final_uri+location.hash};if(result.notices&&result.notices.length){show_status(MESSAGES.read_below,"warn");var click_form=DOM.get("clickthrough_form");var container=click_form.querySelector(".notices");for(var n=0;n<result
2022-05-27 05:41:53 UTC	1037	IN	Data Raw: 65 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 6e 3d 7b 22 41 6d 65 72 69 63 61 2f 44 65 6e 76 65 72 22 3a 5b 22 41 6d 65 72 69 63 61 2f 44 65 6e 76 65 72 22 2c 22 41 6d 65 72 69 63 61 2f 4d 61 7a 61 74 6c 61 6e 22 5d 2c 22 41 6d 65 72 69 63 61 2f 43 68 69 63 61 67 6f 22 3a 5b 22 41 6d 65 72 69 63 61 2f 43 68 69 63 61 67 6f 22 2c 22 41 6d 65 72 69 63 61 2f 4d 65 78 69 63 6f 5f 43 69 74 79 22 5d 2c 22 41 6d 65 72 69 63 61 2f 53 61 6e 74 69 61 67 6f 22 3a 5b 22 41 6d 65 72 69 63 61 2f 53 61 6e 74 69 61 67 6f 22 2c 22 41 6d 65 72 69 63 61 2f 41 73 75 6e 63 69 6f 6e 22 2c 22 41 6d 65 72 69 63 61 2f 43 61 6d 70 6f 5f 47 72 61 6e 64 65 22 5d 2c 22 41 6d 65 72 69 63 61 2f 4d 6f 6e 74 65 76 69 64 65 6f 22 3a 5b 22 41 6d 65 72 69 63 61 2f 4d 6f 6e 74 Data Ascii: e){"use strict";var n={"America/Denver":["America/Denver","America/Mazatlan"],"America/Chicago":["America/Chicago","America/Mexico_City"],"America/Santiago":["America/Santiago","America/Asuncion","America/Campo_Grande"],"America/Montevideo":["America/Mont
2022-05-27 05:41:53 UTC	1043	IN	Data Raw: 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: </html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.3	50026	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:55 UTC	1043	OUT	GET /?locale=de HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: roundcube_cookies=enabled; timezone=America/Los_Angeles; webmailsession=%3aNtsC7AoBd2Q4g_iG%2cbb3e3b737d48efa9ace5acfe9a7f69ad; session_locale=da

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:55 UTC	1043	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:55 GMT Server: Apache Content-Type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 38264 Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: webmailsession=%3aWKtuDfveqf4YKODN%2cb89ee7d54aceca40857f12bddc01d1b9; HttpOnly; path=/; port=443; secure Set-Cookie: session_locale=de; expires=Sat, 27-May-2023 05:41:55 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 0 0:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00 :00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=443; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: imp_key=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00 :00:01 GMT; path=/; port=443 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 27-May-2023 05:41:55 GMT; path=/; port=443; secure Connection: close
2022-05-27 05:41:55 UTC	1045	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 64 65 22 20 64 69 72 3d 22 6c 74 72 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f Data Ascii: <!DOCTYPE html><html lang="de" dir="ltr"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1"> <meta name="goo
2022-05-27 05:41:55 UTC	1051	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 6d 65 73 73 61 67 65 22 3e 54 68 65 20 73 79 73 74 65 6d 20 68 61 73 20 64 65 74 65 63 74 65 64 20 74 68 61 74 20 79 6f 75 20 61 72 65 20 75 73 69 6e 67 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 63 50 61 6e 65 6c 20 26 61 6d 70 3b 20 57 48 4d 20 6e 6f 20 6c 6f 6e 67 65 72 20 73 75 70 70 6f 72 74 73 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 72 65 61 64 20 74 68 65 20 3c 61 20 74 69 74 6c 65 3d 22 63 50 61 6e 65 6c 20 42 6c 6f 67 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6f 2e 63 70 61 6e 65 6c Data Ascii: The system has detected that you are using Internet Explorer 11. cPan el & WHM no longer supports Internet Explorer 11. For more information, read the <a title="cPanel Blog" target="_bla nk" href="https://go.cpanel
2022-05-27 05:41:55 UTC	1053	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 22 3e 73 75 6f 6d 69 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 6c 69 70 69 6e 6f 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 Data Ascii: suomi Filipino
2022-05-27 05:41:55 UTC	1061	IN	Data Raw: d0 b0 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 76 69 27 3e 54 69 e1 ba bf 6e 67 20 56 69 e1 bb 87 74 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 27 3e e4 b8 ad e6 96 87 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 5f 63 6e 27 3e e4 b8 ad e6 96 87 ef bc 88 e4 b8 ad e5 9b bd ef bc 89 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 5f 74 77 27 3e e4 b8 ad e6 96 87 ef bc 88 e5 8f b0 e6 b9 be ef bc 89 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 64 65 27 3e 44 65 75 74 73 63 68 3c 2f 6f 70 74 69 6f 6e 3e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 73 65 6c 65 63 74 3e 0a 20 Data Ascii: </option><option value='vi'>Ting Vit</option><option value='zh'></option><option value='zh_cn'></option> <option value='zh_tw'></option><option value='de'>Deutsch</option> </select>
2022-05-27 05:41:55 UTC	1067	IN	Data Raw: 6f 70 61 63 69 74 79 3d 65 6c 2e 66 69 6c 74 65 72 73 2e 69 74 65 6d 28 22 44 58 49 6d 61 67 65 54 72 61 6e 73 66 6f 72 6d 2e 4d 69 63 72 6f 73 6f 66 74 2e 41 6c 70 68 61 22 29 2e 6f 70 61 63 69 74 79 7d 63 61 74 63 68 28 65 29 7b 74 72 79 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 65 6c 2e 66 69 6c 74 65 72 73 28 22 61 6c 70 68 61 22 29 2e 6f 70 61 63 69 74 79 7d 63 61 74 63 68 28 65 72 72 6f 72 29 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 31 30 30 7d 7d 73 74 61 72 74 5f 6f 70 61 63 69 74 79 2f 3d 31 30 30 7d 69 66 28 21 73 74 61 72 74 5f 6f 70 61 63 69 74 79 29 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 30 7d 7d 65 6c 73 65 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 30 3b 73 65 74 5f 6f 70 61 63 69 74 79 28 65 6c 2c 30 29 7d 69 66 28 5f 66 61 Data Ascii: opacity=el.filters.item("DXImageTransform.Microsoft.Alpha").opacity}catch(e){try{start_opacity=el.filters("a lpha").opacity}catch(error){start_opacity=100}}start_opacity/=100}if(!start_opacity){start_opacity=0}}else{start_opacity =0;set_opacity(el,0)}if(_fa

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:55 UTC	1069	IN	Data Raw: 66 3c 74 6f 70 2e 66 72 61 6d 65 73 2e 6c 65 6e 67 74 68 3b 66 2b 2b 29 7b 69 66 28 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 21 3d 3d 77 69 6e 64 6f 77 29 7b 76 61 72 20 68 72 65 66 3d 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 2e 72 65 70 6c 61 63 65 28 2f 5c 2f 63 70 73 65 73 73 5b 2e 5c 64 5d 2b 2f 2c 72 65 73 75 6c 74 2e 73 65 63 75 72 69 74 79 5f 74 6f 6b 65 6e 29 3b 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 68 72 65 66 7d 7d 6c 6f 63 61 74 69 6f 6e 5f 6f 62 6a 5f 74 6f 5f 72 65 64 69 72 65 63 74 3d 6c 6f 63 61 74 69 6f 6e 7d 76 61 72 20 72 65 64 69 72 65 63 74 6f 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 6c 6f 63 61 74 69 6f 6e 5f 6f 62 6a 5f 74 6f 5f 72 65 64 69 72 65 63 Data Ascii: f<top.frames.length;f++){if(top.frames[f]!==window){var href=top.frames[f].location.href.replace(/\/cpsess[.\d]+/,result.security_token);top.frames[f].location.href=href}}}location_obj_to_redirect=location}var redirector=function(){location_obj_to_redirec
2022-05-27 05:41:55 UTC	1077	IN	Data Raw: 6b 22 3a 74 2c 22 41 73 69 61 2f 49 72 6b 75 74 73 6b 22 3a 74 2c 22 41 73 69 61 2f 59 61 6b 75 74 73 6b 22 3a 74 2c 22 41 73 69 61 2f 56 6c 61 64 69 76 6f 73 74 6f 6b 22 3a 74 2c 22 41 73 69 61 2f 4b 61 6d 63 68 61 74 6b 61 22 3a 74 2c 22 45 75 72 6f 70 65 2f 4d 69 6e 73 6b 22 3a 74 2c 22 41 75 73 74 72 61 6c 69 61 2f 50 65 72 74 68 22 3a 6e 65 77 20 44 61 74 65 28 32 30 30 38 2c 31 30 2c 31 2c 31 2c 30 2c 30 2c 30 29 7d 3b 72 65 74 75 72 6e 20 6e 5b 65 5d 7d 3b 72 65 74 75 72 6e 7b 64 65 74 65 72 6d 69 6e 65 3a 61 2c 64 61 74 65 5f 69 73 5f 64 73 74 3a 6f 2c 64 73 74 5f 73 74 61 72 74 5f 66 6f 72 3a 66 7d 7d 28 29 3b 74 2e 54 69 6d 65 5a 6f 6e 65 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 6e 3d 7b 22 41 6d Data Ascii: k":t,"Asia/Irkutsk":t,"Asia/Yakutsk":t,"Asia/Vladivostok":t,"Asia/Kamchatka":t,"Europe/Minsk":t,"Australia/Perth":new Date(2008,10,1,1,0,0,0)};return n[e]};return{determine:a,date_is_dst:o,dst_start_for:f}}();t.TimeZone=function(e){"use strict";var n={"Am
2022-05-27 05:41:55 UTC	1082	IN	Data Raw: 20 23 73 65 6c 65 63 74 5f 75 73 65 72 5f 66 6f 72 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 70 78 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 70 79 72 69 67 68 74 22 3e 43 6f 70 79 72 69 67 68 74 c2 a9 c2 a0 32 30 32 32 20 63 50 61 6e 65 6c 2c 20 4c 2e 4c 2e 43 2e 0a 20 20 20 20 3c 62 72 20 2f 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6f 2e 63 70 61 6e 65 6c 2e 6e 65 74 2f 70 72 69 76 61 63 79 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 3e 44 61 74 65 6e 73 63 68 75 74 7a 72 69 63 68 74 6c 69 6e 69 65 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 0a 3c 2f 62 6f 64 79 3e 0a 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: #select_user_form { width: px; } }</style> Copyright2022 cPanel, L.L.C. Datenschutzrichtlinie </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.3	50033	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:57 UTC	1083	OUT	GET /?locale=el HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: roundcube_cookies=enabled; timezone=America/Los_Angeles; webmailsession=%3aWKtuDfveqf4YKODN%2cb89ee7d54aceca40857f12bddc01d1b9; session_locale=de
2022-05-27 05:41:57 UTC	1083	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:57 GMT Server: Apache Content-Type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 38890 Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: webmailsession=%3a2Lgd0TyXpGSQwkdE%2cd0b41c879a61f7cb82dc98fec426dd4b; HttpOnly; path=/; port=443; secure Set-Cookie: session_locale=el; expires=Sat, 27-May-2023 05:41:57 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=443; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: imp_key=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 27-May-2023 05:41:57 GMT; path=/; port=443; secure Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:57 UTC	1085	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6c 22 20 64 69 72 3d 22 6c 74 72 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f Data Ascii: <!DOCTYPE html><html lang="el" dir="ltr"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1"> <meta name="goo
2022-05-27 05:41:57 UTC	1091	IN	Data Raw: 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 65 6e 74 2d 77 72 61 70 70 65 72 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 64 65 74 61 69 6c 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 69 63 6f 6e 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 69 63 6f 6e 22 3e 3c 2f 73 70 61 6e 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 6d 65 73 73 61 67 65 22 3e 54 68 65 20 73 79 73 74 65 6d 20 68 61 73 20 64 65 74 65 63 74 65 64 20 74 Data Ascii: <div class="content-wrapper"> <div id="IE-warning-detail"> <div id="IE-warning-icon-container"></div> <div id="IE-warning-message">The system has detected t
2022-05-27 05:41:57 UTC	1093	IN	Data Raw: 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 65 73 5f 34 31 39 22 3e 65 73 70 61 c3 b1 6f 6c 20 6c 61 74 69 6e 6f 61 6d 65 72 69 63 61 6e 6f 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 65 73 5f 65 73 22 3e 65 73 70 61 c3 b1 6f 6c 20 64 65 20 45 73 70 61 c3 b1 61 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 Data Ascii: >espaol latinoamericano</div> <div class="locale-cell">espaol de Espaa</div> <div clas
2022-05-27 05:41:57 UTC	1101	IN	Data Raw: 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 70 74 5f 62 72 27 3e 70 6f 72 74 75 67 75 c3 aa 73 20 64 6f 20 42 72 61 73 69 6c 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 72 6f 27 3e 72 6f 6d c3 a2 6e c4 83 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 72 75 27 3e d1 80 d1 83 d1 81 d1 81 d0 ba d0 b8 d0 b9 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 73 6c 27 3e 73 6c 6f 76 65 6e c5 a1 c4 8d 69 6e 61 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 73 76 27 3e 73 76 65 6e 73 6b 61 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 74 68 27 3e e0 b9 84 e0 b8 97 e0 b8 a2 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f Data Ascii: option><option value='pt_br'>portugus do Brasil</option><option value='ro'>romn</option><option value='ru'></option><option value='sl'>slovenina</option><option value='sv'>svenska</option><option value='th'></option><optio
2022-05-27 05:41:57 UTC	1107	IN	Data Raw: 73 68 6f 77 5f 6c 6f 63 61 6c 65 73 3f 66 61 64 65 5f 6f 75 74 3a 66 61 64 65 5f 69 6e 29 28 22 6c 6f 63 61 6c 65 2d 66 6f 6f 74 65 72 22 29 7d 66 75 6e 63 74 69 6f 6e 20 73 68 6f 77 49 45 42 61 6e 6e 65 72 28 29 7b 69 66 28 6e 61 76 69 67 61 74 6f 72 2e 75 73 65 72 41 67 65 6e 74 2e 69 6e 64 65 78 4f 66 28 22 54 72 69 64 65 6e 74 22 29 21 3d 3d 2d 31 29 7b 76 61 72 20 69 65 42 61 6e 6e 65 72 44 69 76 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 49 45 2d 77 61 72 6e 69 6e 67 22 29 3b 69 66 28 69 65 42 61 6e 6e 65 72 44 69 76 29 7b 69 65 42 61 6e 6e 65 72 44 69 76 2e 63 6c 61 73 73 4c 69 73 74 2e 72 65 6d 6f 76 65 28 22 49 45 2d 77 61 72 6e 69 6e 67 2d 68 69 64 65 22 29 7d 7d 7d 73 68 6f 77 49 45 42 61 6e 6e 65 72 28 29 Data Ascii: show_locales?fade_out:fade_in)("locale-footer")}function showIEBanner(){if(navigator.userAgent.indexOf("Trident")!==-1){var ieBannerDiv=document.getElementById("IE-warning");if(ieBannerDiv){ieBannerDiv.classList.remove("IE-warning-hide")}}}showIEBanner()
2022-05-27 05:41:57 UTC	1109	IN	Data Raw: 68 69 73 2e 5f 75 72 6c 2b 22 3f 22 2b 70 61 73 73 44 61 74 61 2b 22 26 74 69 6d 65 73 74 61 6d 70 3d 22 2b 28 6e 65 77 20 44 61 74 65 29 2e 67 65 74 54 69 6d 65 28 29 3b 61 6a 61 78 2e 6f 70 65 6e 28 22 47 45 54 22 2c 75 72 69 2c 74 72 75 65 29 3b 61 6a 61 78 2e 73 65 6e 64 28 6e 75 6c 6c 29 7d 74 68 69 73 2e 41 4a 41 58 3d 61 6a 61 78 3b 74 68 69 73 2e 75 70 64 61 74 69 6e 67 3d 74 72 75 65 7d 63 61 74 63 68 28 65 29 7b 6c 6f 67 69 6e 5f 66 6f 72 6d 2e 73 75 62 6d 69 74 28 29 7d 72 65 74 75 72 6e 20 74 72 75 65 7d 3b 76 61 72 20 5f 74 65 78 74 5f 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 43 6f 6e 74 65 6e 74 22 69 6e 20 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 3f 22 74 65 78 74 43 6f 6e 74 65 6e 74 22 3a 22 69 6e 6e 65 72 54 65 78 74 22 3b 66 75 6e 63 74 69 Data Ascii: his._url+"?"+passData+"&timestamp="+(new Date).getTime();ajax.open("GET",uri,true);ajax.send(null)}this.AJAX=ajax;this.updating=true}catch(e){login_form.submit()}return true};var _text_content="textContent"in document.body?"textContent":"innerText";functi
2022-05-27 05:41:57 UTC	1117	IN	Data Raw: 32 30 31 31 2c 32 2c 32 37 2c 31 2c 30 2c 30 2c 30 29 2c 22 45 75 72 6f 70 65 2f 48 65 6c 73 69 6e 6b 69 22 3a 6e 65 77 20 44 61 74 65 28 32 30 31 31 2c 32 2c 32 37 2c 34 2c 30 2c 30 2c 30 29 2c 22 45 75 72 6f 70 65 2f 49 73 74 61 6e 62 75 6c 22 3a 6e 65 77 20 44 61 74 65 28 32 30 31 31 2c 32 2c 32 38 2c 35 2c 30 2c 30 2c 30 29 2c 22 41 73 69 61 2f 44 61 6d 61 73 63 75 73 22 3a 6e 65 77 20 44 61 74 65 28 32 30 31 31 2c 33 2c 31 2c 32 2c 30 2c 30 2c 30 29 2c 22 41 73 69 61 2f 4a 65 72 75 73 61 6c 65 6d 22 3a 6e 65 77 20 44 61 74 65 28 32 30 31 31 2c 33 2c 31 2c 36 2c 30 2c 30 2c 30 29 2c 22 41 73 69 61 2f 47 61 7a 61 22 3a 6e 65 77 20 44 61 74 65 28 32 30 30 39 2c 32 2c 32 38 2c 30 2c 33 30 2c 30 2c 30 29 2c 22 41 66 72 69 63 61 2f 43 61 69 72 6f 22 3a 6e Data Ascii: 2011,2,27,1,0,0,0),"Europe/Helsinki":new Date(2011,2,27,4,0,0,0),"Europe/Istanbul":new Date(2011,2,28,5,0,0,0),"Asia/Damascus":new Date(2011,3,1,2,0,0,0),"Asia/Jerusalem":new Date(2011,3,1,6,0,0,0),"Asia/Gaza":new Date(2009,2,28,0,30,0,0),"Africa/Cairo":n
2022-05-27 05:41:57 UTC	1122	IN	Data Raw: 29 7b 76 61 72 20 64 65 74 65 63 74 65 64 5f 6e 6f 64 65 73 3d 64 6f 63 75 6d 65 6e 74 2e 71 75 65 72 79 53 65 6c 65 63 74 6f 72 41 6c 6c 28 22 2e 22 2b 44 45 54 45 43 54 45 44 5f 54 5a 5f 43 4c 41 53 53 29 3b 5b 5d 2e 66 6f 72 45 61 63 68 2e 63 61 6c 6c 28 64 65 74 65 63 74 65 64 5f 6e 6f 64 65 73 2c 28 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 6e 2e 74 65 78 74 43 6f 6e 74 65 6e 74 3d 64 65 74 65 63 74 65 64 5f 74 7a 7d 29 29 3b 76 61 72 20 73 68 6f 77 5f 6e 6f 64 65 73 3d 64 6f 63 75 6d 65 6e 74 2e 71 75 65 72 79 53 65 6c 65 63 74 6f 72 41 6c 6c 28 22 2e 22 2b 43 4f 4f 4b 49 45 5f 54 49 4d 45 5a 4f 4e 45 5f 4d 49 53 4d 41 54 43 48 5f 43 4c 41 53 53 29 3b 5b 5d 2e 66 6f 72 45 61 63 68 2e 63 61 6c 6c 28 73 68 6f 77 5f 6e 6f 64 65 73 2c 28 66 75 6e 63 74 69 6f Data Ascii:){var detected_nodes=document.querySelectorAll("."+DETECTED_TZ_CLASS);[].forEach.call(detected_nodes,(function(n){n.textContent=detected_tz}));var show_nodes=document.querySelectorAll("."+COOKIE_TIMEZONE_MISMATCH_CLASS);[].forEach.call(show_nodes,(functio

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	50038	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:42:01 UTC	1123	OUT	GET /?locale=es HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183. 121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig ned-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: roundcube_cookies=enabled; timezone=America/Los_Angeles; webmailsession=%3a2Lgd0TyXpGSQwkdE% 2cd0b41c879a61f7cb82dc98fec426dd4b; session_locale=el
2022-05-27 05:42:01 UTC	1124	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:42:01 GMT Server: Apache Content-Type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 38348 Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: webmailsession=%3aKk4R4ZDdfAW0yFSx%2c920b5fb218bef83b478ad693450ddb27; HttpOnly; path=/; port=443; secure Set-Cookie: session_locale=es; expires=Sat, 27-May-2023 05:42:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 0 0:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00 :00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=443; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: imp_key=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00 :00:01 GMT; path=/; port=443 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 27-May-2023 05:42:01 GMT; path=/; port=443; secure Connection: close
2022-05-27 05:42:01 UTC	1126	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 73 22 20 64 69 72 3d 22 6c 74 72 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f Data Ascii: <!DOCTYPE html><html lang="es" dir="ltr"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user- scalable=1"> <meta name="goo
2022-05-27 05:42:01 UTC	1132	IN	Data Raw: 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 6d 65 73 73 61 67 65 22 3e 54 68 65 20 73 79 73 74 65 6d 20 68 61 73 20 64 65 74 65 63 74 65 64 20 74 68 61 74 20 79 6f 75 20 61 72 65 20 75 73 69 6e 67 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 63 50 61 6e 65 6c 20 26 61 6d 70 3b 20 57 48 4d 20 6e 6f 20 6c 6f 6e 67 65 72 20 73 75 70 70 6f 72 74 73 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 72 65 61 64 20 74 68 65 20 3c 61 20 74 69 74 6c 65 3d 22 63 50 61 6e 65 6c 20 42 6c 6f 67 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6f 2e 63 70 61 6e 65 6c 2e 6e 65 74 2f 69 Data Ascii: <div id="IE-warning-message">The system has detected that you are using Internet Explorer 11. cPanel & WHM no longer supports Internet Explorer 11. For more information, read the <a title="cPanel Blog" target=" _blank" href="https://go.cpanel.net/i
2022-05-27 05:42:01 UTC	1134	IN	Data Raw: 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 22 3e 73 75 6f 6d 69 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 6c 22 3e 46 69 6c 69 70 69 6e 6f 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 Data Ascii: <div class="locale-cell">suomi</div> <div class="locale-cell">Filipino</div>

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:42:01 UTC	1142	IN	Data Raw: c3 bc 72 6b c3 a7 65 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 75 6b 27 3e d1 83 d0 ba d1 80 d0 b0 d1 97 d0 bd d1 81 d1 8c d0 ba d0 b0 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 76 69 27 3e 54 69 e1 ba bf 6e 67 20 56 69 e1 bb 87 74 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 27 3e e4 b8 ad e6 96 87 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 5f 63 6e 27 3e e4 b8 ad e6 96 87 ef bc 88 e4 b8 ad e5 9b bd ef bc 89 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 5f 74 77 27 3e e4 b8 ad e6 96 87 ef bc 88 e5 8f b0 e6 b9 be ef bc 89 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 65 73 Data Ascii: rke</option><option value='uk'></option><option value='vi'>Ting Vit</option><option value='zh'></option><option value='zh_cn'></option><option value='zh_tw'></option><option value='es
2022-05-27 05:42:01 UTC	1147	IN	Data Raw: 69 64 64 65 6e 22 29 7b 69 66 28 77 69 6e 64 6f 77 2e 67 65 74 43 6f 6d 70 75 74 65 64 53 74 79 6c 65 29 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 4e 75 6d 62 65 72 28 63 75 72 5f 73 74 79 6c 65 2e 6f 70 61 63 69 74 79 29 7d 65 6c 73 65 7b 74 72 79 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 65 6c 2e 66 69 6c 74 65 72 73 2e 69 74 65 6d 28 22 44 58 49 6d 61 67 65 54 72 61 6e 73 66 6f 72 6d 2e 4d 69 63 72 6f 73 6f 66 74 2e 41 6c 70 68 61 22 29 2e 6f 70 61 63 69 74 79 7d 63 61 74 63 68 28 65 29 7b 74 72 79 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 65 6c 2e 66 69 6c 74 65 72 73 28 22 61 6c 70 68 61 22 29 2e 6f 70 61 63 69 74 79 7d 63 61 74 63 68 28 65 72 72 6f 72 29 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 31 30 30 7d 7d 73 74 61 72 74 5f 6f 70 61 Data Ascii: idden"){if(window.getComputedStyle){start_opacity=Number(cur_style.opacity)}else{try{start_opacity=el.filters.item("DXImageTransform.Microsoft.Alpha").opacity}catch(e){try{start_opacity=el.filters("alpha").opacity}catch(error){start_opacity=100}}start_opa
2022-05-27 05:42:01 UTC	1150	IN	Data Raw: 74 69 6f 6e 5f 6f 62 6a 5f 74 6f 5f 72 65 64 69 72 65 63 74 3d 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 7d 65 6c 73 65 7b 69 66 28 72 65 73 75 6c 74 2e 73 65 63 75 72 69 74 79 5f 74 6f 6b 65 6e 26 26 74 6f 70 21 3d 3d 77 69 6e 64 6f 77 29 7b 66 6f 72 28 76 61 72 20 66 3d 30 3b 66 3c 74 6f 70 2e 66 72 61 6d 65 73 2e 6c 65 6e 67 74 68 3b 66 2b 2b 29 7b 69 66 28 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 21 3d 3d 77 69 6e 64 6f 77 29 7b 76 61 72 20 68 72 65 66 3d 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 2e 72 65 70 6c 61 63 65 28 2f 5c 2f 63 70 73 65 73 73 5b 2e 5c 64 5d 2b 2f 2c 72 65 73 75 6c 74 2e 73 65 63 75 72 69 74 79 5f 74 6f 6b 65 6e 29 3b 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 Data Ascii: tion_obj_to_redirect=top.location}else{if(result.security_token&&top!==window){for(var f=0;f<top.frames.length;f++){if(top.frames[f]!==window){var href=top.frames[f].location.href.replace(/\/cpsess[.\d]+/,result.security_token);top.frames[f].location.href
2022-05-27 05:42:01 UTC	1158	IN	Data Raw: 28 32 30 31 31 2c 32 2c 32 37 2c 31 2c 30 2c 30 2c 30 29 2c 22 45 75 72 6f 70 65 2f 4d 6f 73 63 6f 77 22 3a 74 2c 22 41 73 69 61 2f 59 65 6b 61 74 65 72 69 6e 62 75 72 67 22 3a 74 2c 22 41 73 69 61 2f 4f 6d 73 6b 22 3a 74 2c 22 41 73 69 61 2f 4b 72 61 73 6e 6f 79 61 72 73 6b 22 3a 74 2c 22 41 73 69 61 2f 49 72 6b 75 74 73 6b 22 3a 74 2c 22 41 73 69 61 2f 59 61 6b 75 74 73 6b 22 3a 74 2c 22 41 73 69 61 2f 56 6c 61 64 69 76 6f 73 74 6f 6b 22 3a 74 2c 22 41 73 69 61 2f 4b 61 6d 63 68 61 74 6b 61 22 3a 74 2c 22 45 75 72 6f 70 65 2f 4d 69 6e 73 6b 22 3a 74 2c 22 41 75 73 74 72 61 6c 69 61 2f 50 65 72 74 68 22 3a 6e 65 77 20 44 61 74 65 28 32 30 30 38 2c 31 30 2c 31 2c 31 2c 30 2c 30 2c 30 29 7d 3b 72 65 74 75 72 6e 20 6e 5b 65 5d 7d 3b 72 65 74 75 72 6e 7b 64 Data Ascii: (2011,2,27,1,0,0,0),"Europe/Moscow":t,"Asia/Yekaterinburg":t,"Asia/Omsk":t,"Asia/Krasnoyarsk":t,"Asia/Irkutsk":t,"Asia/Yakutsk":t,"Asia/Vladivostok":t,"Asia/Kamchatka":t,"Europe/Minsk":t,"Australia/Perth":new Date(2008,10,1,1,0,0,0)};return n[e]};return{d
2022-05-27 05:42:01 UTC	1163	IN	Data Raw: 3b 0a 0a 0a 43 50 54 69 6d 65 7a 6f 6e 65 2e 72 65 73 65 74 5f 74 69 6d 65 7a 6f 6e 65 28 29 3b 0a 3c 2f 73 63 72 69 70 74 3e 0a 0a 3c 73 74 79 6c 65 3e 0a 20 20 20 20 40 6d 65 64 69 61 20 28 6d 69 6e 2d 77 69 64 74 68 3a 20 34 38 31 70 78 29 20 7b 0a 20 20 20 20 20 20 20 20 23 73 65 6c 65 63 74 5f 75 73 65 72 5f 66 6f 72 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 70 78 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 70 79 72 69 67 68 74 22 3e 43 6f 70 79 72 69 67 68 74 c2 a9 c2 a0 32 30 32 32 20 63 50 61 6e 65 6c 2c 20 4c 2e 4c 2e 43 2e 0a 20 20 20 20 3c 62 72 20 2f 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6f 2e 63 70 61 6e 65 Data Ascii: ;CPTimezone.reset_timezone();</script><style> @media (min-width: 481px) { #select_user_form { width: px; } }</style> Copyright2022 cPanel, L.L.C. <a href="https://go.cpane

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	50044	103.6.196.136	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:42:05 UTC	1163	OUT	GET /?locale=es_419 HTTP/1.1 Host: webmail.serendahsteel.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: roundcube_cookies=enabled; timezone=America/Los_Angeles; webmailsession=%3aKk4R4ZDdfAW0yFSx%2c920b5fb218bef83b478ad693450ddb27; session_locale=es

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:42:05 UTC	1164	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:42:05 GMT Server: Apache Content-Type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 38347 Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: webmailsession=%3ahLAQZKnz6ABm0gLS%2c5d24227aa68311b58263b1fe625c7181; HttpOnly; path=/; port=443; secure Set-Cookie: session_locale=es_419; expires=Sat, 27-May-2023 05:42:05 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 0 0:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00 :00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=443; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: imp_key=expired; HttpOnly; domain=webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.serendahsteel.com; expires=Thu, 01-Jan-1970 00 :00:01 GMT; path=/; port=443 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 27-May-2023 05:42:05 GMT; path=/; port=443; secure Connection: close
2022-05-27 05:42:05 UTC	1166	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 73 5f 34 31 39 22 20 64 69 72 3d 22 6c 74 72 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d Data Ascii: <!DOCTYPE html><html lang="es_419" dir="ltr"><head> <meta http-equiv="Content-Type" content="te xt/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, u ser-scalable=1"> <meta name=
2022-05-27 05:42:05 UTC	1172	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 49 45 2d 77 61 72 6e 69 6e 67 2d 6d 65 73 73 61 67 65 22 3e 54 68 65 20 73 79 73 74 65 6d 20 68 61 73 20 64 65 74 65 63 74 65 64 20 74 68 61 74 20 79 6f 75 20 61 72 65 20 75 73 69 6e 67 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 63 50 61 6 e 65 6c 20 26 61 6d 70 3b 20 57 48 4d 20 6e 6f 20 6c 6f 6e 67 65 72 20 73 75 70 70 6f 72 74 73 20 49 6e 74 65 72 6e 65 74 20 45 78 70 6c 6f 72 65 72 20 31 31 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 72 65 61 64 20 74 68 65 20 3c 61 20 74 69 74 6c 65 3d 22 63 50 61 6e 65 6c 20 42 6c 6f 67 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6f 2e Data Ascii: <div id="IE-warning-message">The system has detected that you are using Internet Explorer 11. cPanel & WHM no longer supports Internet Explorer 11. For more information, read the <a title="cPanel Blog" target ="_blank" href="https://go.
2022-05-27 05:42:06 UTC	1174	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 61 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 22 3e 73 75 6f 6d 69 3c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 63 6 1 6c 65 2d 63 65 6c 6c 22 3e 3c 61 20 68 72 65 66 3d 22 3f 6c 6f 63 61 6c 65 3d 66 69 6c 22 3e 46 69 6c 69 70 69 6e 6f 3 c 2f 61 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 Data Ascii: <div class="locale-cell">suomi</div> <div class="locale-cell">Filipino</div>
2022-05-27 05:42:06 UTC	1182	IN	Data Raw: 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 75 6b 27 3e d1 83 d0 ba d1 80 d0 b0 d1 97 d0 bd d1 81 d1 8c d0 ba d0 b0 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 76 69 27 3e 54 69 e1 ba bf 6e 67 20 56 69 e1 bb 87 74 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 27 3e e4 b8 ad e6 96 87 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 5f 63 6e 27 3e e4 b8 ad e6 96 87 ef bc 88 e4 b8 ad e5 9b bd ef bc 89 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 7a 68 5f 74 77 27 3e e4 b8 ad e6 96 87 ef bc 88 e5 8f b0 e6 b9 be ef bc 89 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 27 65 73 5f 34 31 39 27 3e 65 73 70 61 c3 b1 Data Ascii: ion><option value='uk'></option><option value='vi'>Ting Vit</option><option value='zh'></option><option valu e='zh_cn'></option><option value='zh_tw'></option><option value='es_419'>espa
2022-05-27 05:42:06 UTC	1187	IN	Data Raw: 3d 22 68 69 64 64 65 6e 22 29 7b 69 66 28 77 69 6e 64 6f 77 2e 67 65 74 43 6f 6d 70 75 74 65 64 53 74 79 6c 65 29 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 4e 75 6d 62 65 72 28 63 75 72 5f 73 74 79 6c 65 2e 6f 70 61 63 69 74 79 29 7d 65 6c 73 65 7b 74 72 79 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 65 6c 2e 66 69 6c 74 65 72 73 2e 69 74 65 6d 28 22 44 58 49 6d 61 67 65 54 72 61 6e 73 66 6f 72 6d 2e 4d 69 63 72 6f 73 6f 66 74 2e 41 6c 70 68 61 22 29 2e 6f 70 61 63 69 74 79 7d 63 61 74 63 68 28 65 29 7b 74 72 79 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 65 6c 2e 66 69 6c 74 65 72 73 28 22 61 6c 70 68 61 22 29 2e 6f 70 61 63 69 74 79 7d 63 61 74 63 68 28 65 72 72 6f 72 29 7b 73 74 61 72 74 5f 6f 70 61 63 69 74 79 3d 31 30 30 7d 7d 73 74 61 72 74 5f Data Ascii: ="hidden"){if(window.getComputedStyle){start_opacity=Number(cur_style.opacity)}else{try{start_opacity=el.fil ters.item("DXImageTransform.Microsoft.Alpha").opacity}catch(e){try{start_opacity=el.filters("alpha").opacity}catch(error) {start_opacity=100}}start_

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:42:06 UTC	1190	IN	Data Raw: 69 6f 6e 5f 6f 62 6a 5f 74 6f 5f 72 65 64 69 72 65 63 74 3d 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 7d 65 6c 73 65 7b 69 66 28 72 65 73 75 6c 74 2e 73 65 63 75 72 69 74 79 5f 74 6f 6b 65 6e 26 26 74 6f 70 21 3d 3d 77 69 6e 64 6f 77 29 7b 66 6f 72 28 76 61 72 20 66 3d 30 3b 66 3c 74 6f 70 2e 66 72 61 6d 65 73 2e 6c 65 6e 67 74 68 3b 66 2b 2b 29 7b 69 66 28 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 21 3d 3d 77 69 6e 64 6f 77 29 7b 76 61 72 20 68 72 65 66 3d 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 2e 72 65 70 6c 61 63 65 28 2f 5c 2f 63 70 73 65 73 73 5b 2e 5c 64 5d 2b 2f 2c 72 65 73 75 6c 74 2e 73 65 63 75 72 69 74 79 5f 74 6f 6b 65 6e 29 3b 74 6f 70 2e 66 72 61 6d 65 73 5b 66 5d 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d Data Ascii: ion_obj_to_redirect=top.location}else{if(result.security_token&&top!==window){for(var f=0;f<top.frames.lengt h;f++){if(top.frames[f]!==window){var href=top.frames[f].location.href.replace(/\/cpsess[.\d]+/,result.security_token);t op.frames[f].location.href=
2022-05-27 05:42:06 UTC	1198	IN	Data Raw: 32 30 31 31 2c 32 2c 32 37 2c 31 2c 30 2c 30 2c 30 29 2c 22 45 75 72 6f 70 65 2f 4d 6f 73 63 6f 77 22 3a 74 2c 22 41 73 69 61 2f 59 65 6b 61 74 65 72 69 6e 62 75 72 67 22 3a 74 2c 22 41 73 69 61 2f 4f 6d 73 6b 22 3a 74 2c 22 41 73 69 61 2f 4b 72 61 73 6e 6f 79 61 72 73 6b 22 3a 74 2c 22 41 73 69 61 2f 49 72 6b 75 74 73 6b 22 3a 74 2c 22 41 73 69 61 2f 59 61 6b 75 74 73 6b 22 3a 74 2c 22 41 73 69 61 2f 56 6c 61 64 69 76 6f 73 74 6f 6b 22 3a 74 2c 22 41 73 69 61 2f 4b 61 6d 63 68 61 74 6b 61 22 3a 74 2c 22 45 75 72 6f 70 65 2f 4d 69 6e 73 6b 22 3a 74 2c 22 41 75 73 74 72 61 6c 69 61 2f 50 65 72 74 68 22 3a 6e 65 77 20 44 61 74 65 28 32 30 30 38 2c 31 30 2c 31 2c 31 2c 30 2c 30 2c 30 29 7d 3b 72 65 74 75 72 6e 20 6e 5b 65 5d 7d 3b 72 65 74 75 72 6e 7b 64 65 Data Ascii: 2011,2,27,1,0,0,0),"Europe/Moscow":t,"Asia/Yekaterinburg":t,"Asia/Omsk":t,"Asia/Krasnoyarsk":t,"Asia/Irkutsk ":t,"Asia/Yakutsk":t,"Asia/Vladivostok":t,"Asia/Kamchatka":t,"Europe/Minsk":t,"Australia/Perth":new Date(2008,10,1,1,0,0 ,0)};return n[e]};return{de
2022-05-27 05:42:06 UTC	1203	IN	Data Raw: 6f 77 29 3b 0a 0a 0a 43 50 54 69 6d 65 7a 6f 6e 65 2e 72 65 73 65 74 5f 74 69 6d 65 7a 6f 6e 65 28 29 3b 0a 3c 2f 73 63 72 69 70 74 3e 0a 0a 3c 73 74 79 6c 65 3e 0a 20 20 20 20 40 6d 65 64 69 61 20 28 6d 69 6e 2d 77 69 64 74 68 3a 20 34 38 31 70 78 29 20 7b 0a 20 20 20 20 20 20 20 20 23 73 65 6c 65 63 74 5f 75 73 65 72 5f 66 6f 72 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 70 78 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 70 79 72 69 67 68 74 22 3e 43 6f 70 79 72 69 67 68 74 c2 a9 c2 a0 32 30 32 32 20 63 50 61 6e 65 6c 2c 20 4c 2e 4c 2e 43 2e 0a 20 20 20 20 3c 62 72 20 2f 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6f 2e 63 70 Data Ascii: ow);CPTimezone.reset_timezone();</script><style> @media (min-width: 481px) { #select_user_form { width: px; } }</style> Copyright2022 cPanel, L.L.C. <a href="https://go.cp

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49828	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:07 UTC	138	OUT	GET /cPanel_magic_revision_1458739301/unprotected/cpanel/images/webmail-logo.svg HTTP/1.1 Host: webmail.unitedyacht.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183. 121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://arthurperush.com/css/cPanel.SharePoint_documentOnline/login.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 05:41:07 UTC	190	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:07 GMT Server: Apache/2.4.53 (cPanel) OpenSSL/1.1.1o mod_bwlimited/1.4 Content-Type: image/svg+xml Last-Modified: Wed, 16 Jan 2019 19:01:25 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:07 GMT Content-Length: 5360 Vary: Accept-Encoding,User-Agent Connection: close
2022-05-27 05:41:07 UTC	190	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 34 36 32 70 74 22 20 68 65 69 67 68 74 3d 22 33 32 30 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 34 36 32 20 32 34 30 22 3e 3c 64 65 66 73 3e 3c 63 6c 69 70 50 61 74 68 20 69 64 3d 22 61 22 3e 3c 70 61 74 68 20 64 3d 22 4d 31 33 33 39 20 30 68 31 32 32 2e 34 34 76 32 34 30 48 31 33 33 39 7a 6d 30 20 30 22 2f 3e 3c 2f 63 6c 69 70 50 61 74 68 3e 3c 2f 64 65 66 73 3e 3c 70 61 74 68 20 64 3d 22 4d 33 36 35 2e 31 30 32 20 31 34 2e 33 39 38 6c 2d 34 33 2e 32 30 34 20 31 36 30 2e 32 30 34 63 2d 32 2e 35 39 37 20 39 2e 35 39 37 2d 36 2e 35 39 37 20 31 38 2e 34 35 2d 31 32 20 32 36 2e 35 34 36 2d 35 2e 33 39 38 20 38 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="1462pt" height="320" viewBox="0 0 1462 240"><defs>< clipPath id="a"><path d="M1339 0h122.44v240H1339zm0 0"/></clipPath></defs><path d="M365.102 14.398l-43.204 160 .204c-2.597 9.597-6.597 18.45-12 26.546-5.398 8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49829	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:07 UTC	195	OUT	GET /cPanel_magic_revision_1547665285/unprotected/cpanel/images/icon-username.png HTTP/1.1 Host: webmail.unitedyacht.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://webmail.unitedyacht.com/cPanel_magic_revision_1508464910/unprotected/cpanel/style_v2_optimized.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 05:41:08 UTC	201	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:08 GMT Server: Apache/2.4.53 (cPanel) OpenSSL/1.1.1o mod_bwlimited/1.4 Content-Type: image/png Last-Modified: Wed, 16 Jan 2019 19:01:25 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:08 GMT Content-Length: 320 Connection: close
2022-05-27 05:41:08 UTC	201	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 14 00 00 00 14 08 06 00 00 00 8d 89 1d 0d 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 88 00 00 00 09 70 48 59 73 00 00 0b 12 00 00 0b 12 01 d2 dd 7e fc 00 00 00 1c 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 46 69 72 65 77 6f 72 6b 73 20 43 53 34 06 b2 d3 a0 00 00 00 01 5 74 45 58 74 43 72 65 61 74 69 6f 6e 20 54 69 6d 65 00 36 2f 32 39 2f 31 31 13 6b 0a 4d 00 00 00 99 49 44 41 54 38 cb 63 f8 ff ff 3f 03 35 31 82 81 06 d8 6c 3c d9 81 d8 0a 88 e3 80 b8 18 4a cb 82 c4 41 f2 e4 18 18 0e 35 08 1d 87 93 6b 60 31 2e 3c 0c 0d 04 6a 32 c6 67 20 48 9e 54 03 ad 08 18 68 45 aa 81 2a 78 0c cb 01 c9 93 13 86 b8 5c a9 4d 6e a4 b0 23 25 6a 18 8e 83 c9 93 6c 20 0e 57 5a 51 6a a0 3f 9a 81 fe 24 1b 08 8d Data Ascii: PNGIHDRsBIT|dpHYs~tEXtSoftwareAdobe Fireworks CS4tEXtCreation Time6/29/11kMIDAT8c?51l<JA5k`1.<j2g HThE*x\Mn#%jl WZQj?$

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49830	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:07 UTC	196	OUT	GET /cPanel_magic_revision_1547665285/unprotected/cpanel/images/icon-password.png HTTP/1.1 Host: webmail.unitedyacht.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://webmail.unitedyacht.com/cPanel_magic_revision_1508464910/unprotected/cpanel/style_v2_optimized.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 05:41:08 UTC	201	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:08 GMT Server: Apache/2.4.53 (cPanel) OpenSSL/1.1.1o mod_bwlimited/1.4 Content-Type: image/png Last-Modified: Wed, 16 Jan 2019 19:01:25 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:08 GMT Content-Length: 450 Connection: close
2022-05-27 05:41:08 UTC	202	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 14 00 00 00 14 08 06 00 00 00 8d 89 1d 0d 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 88 00 00 00 09 70 48 59 73 00 00 0b 12 00 00 0b 12 01 d2 dd 7e fc 00 00 00 1c 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 46 69 72 65 77 6f 72 6b 73 20 43 53 34 06 b2 d3 a0 00 00 00 01 5 74 45 58 74 43 72 65 61 74 69 6f 6e 20 54 69 6d 65 00 36 2f 32 39 2f 31 31 13 6b 0a 4d 00 00 01 1b 49 44 41 54 38 cb 63 f8 ff ff 3f 03 35 31 2a 07 09 b0 d9 78 b2 03 b1 15 10 e7 00 71 31 14 a7 82 c4 40 f2 24 19 08 32 8c dd d6 2b 0e 64 88 80 4b 60 92 7e 4c ba 2b 08 0b bb 07 c7 40 0d f6 27 c9 40 0e 5b 2f 47 90 46 97 dc 32 2b a0 b8 30 10 f3 40 b1 20 48 0c 6a a8 15 29 2e 2c 96 f6 89 08 07 8a 71 32 a0 01 90 98 42 60 4c 20 a7 Data Ascii: PNGIHDRsBIT|dpHYs~tEXtSoftwareAdobe Fireworks CS4tEXtCreation Time6/29/11kMIDAT8c?51*xq1 @$2+dK`~L+@'@[/GF2+0@ Hj).,q2B`L

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49832	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:07 UTC	196	OUT	GET /cPanel_magic_revision_1616517441/unprotected/cpanel/fonts/open_sans/OpenSans-Regular-webfont.woff HTTP/1.1 Host: webmail.unitedyacht.com Connection: keep-alive Origin: https://arthurperush.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: font Referer: https://webmail.unitedyacht.com/cPanel_magic_revision_1386192030/unprotected/cpanel/fonts/open_sans/open_sans.min.css Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 05:41:08 UTC	202	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:08 GMT Server: Apache/2.4.53 (cPanel) OpenSSL/1.1.1o mod_bwlimited/1.4 Content-Type: application/font-woff Last-Modified: Tue, 23 Mar 2021 16:37:21 GMT Cache-Control: max-age=5184000, public Expires: Tue, 26 Jul 2022 05:41:08 GMT Content-Length: 22660 Vary: Accept-Encoding,User-Agent Connection: close
2022-05-27 05:41:08 UTC	203	IN	Data Raw: 77 4f 46 46 00 01 00 00 00 00 58 84 00 13 00 00 00 00 95 58 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 46 46 54 4d 00 00 01 a8 00 00 00 1c 00 00 00 1c 63 47 ec 8f 47 44 45 46 00 00 01 c4 00 00 00 1e 00 00 00 20 01 1d 00 04 47 50 4f 53 00 00 01 e4 00 00 04 a3 00 00 09 9e 2d 72 17 42 47 53 55 42 00 00 06 88 00 00 00 81 00 00 00 a8 a0 63 88 a1 4f 53 2f 32 00 00 07 0c 00 00 00 60 00 00 00 60 a0 e5 99 7f 63 6d 61 70 00 00 07 6c 00 00 01 a2 00 00 02 0a 13 f0 34 51 63 76 74 20 00 00 09 10 00 00 00 30 00 00 00 3c 29 c6 06 3b 66 70 67 6d 00 00 09 40 00 00 04 fa 00 00 09 91 8b 0b 7a 41 67 61 73 70 00 00 0e 3c 00 00 00 08 00 00 00 08 00 00 00 10 67 6c 79 66 00 00 0e 44 00 00 41 3e 00 00 6f 70 52 6a bc 2d 68 65 61 64 00 00 4f 84 00 00 00 Data Ascii: wOFFXXFFTMcGGDEF GPOS-rBGSUBcOS/2``cmapl4Qcvt 0<);fpgm@zAgasp<glyfDA>opRj-headO
2022-05-27 05:41:08 UTC	210	IN	Data Raw: ac a3 46 c9 b2 e5 bd c6 51 d2 a1 eb fd 44 e0 ad b0 6f e7 f1 6b df 87 f8 20 b1 5c 88 85 cb 33 78 62 83 d5 05 06 51 43 e5 da 2a 3b 18 30 75 95 35 70 00 2c 9d 14 c0 52 17 bd da f8 89 ce b2 fd 15 21 51 47 cc e4 09 f1 cc 87 0d 8d 27 00 4c 97 04 ec 2d 12 fa a8 fe 1e 93 f3 e3 bf 37 9e 45 6e 55 7e 53 50 64 3c 2b 1d a7 db e9 eb 4c d9 e0 d1 10 71 74 c5 63 af 4f 0f 7e f7 9f 9f 7f fa fe 3f 41 88 6b 9f a4 f7 82 14 57 e3 09 78 39 bd 8f ee a0 17 e8 db 38 07 b7 83 d8 36 9b aa f9 6b b6 de d5 7c df da b4 9d 0b 62 84 58 f4 c7 f7 56 28 a4 4a 73 bb ad a9 3c 1d 2a ba 79 38 95 82 fd 9a 56 16 ab e9 39 fa c5 de 7a 3c 97 a4 05 a3 36 7f fa d6 f1 d3 c7 45 e3 df ff 1d 04 7a 83 09 eb 9e 5c bb 9a d3 4a 77 71 5a a3 61 57 43 e4 0b ab 26 30 8f 1f a3 c9 21 50 dc 17 09 7b e8 10 91 f0 f4 ab Data Ascii: FQDok \3xbQC*;0u5p,R!QG'L-7EnU~SPd<+LqtcO~?AkWx986k|bXV(Js<*y8V9z<6Ez\JwqZaWC&0!P{

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49831	72.9.144.117	443	C:\Program Files\Google\Chrome\Application\chrome.exe

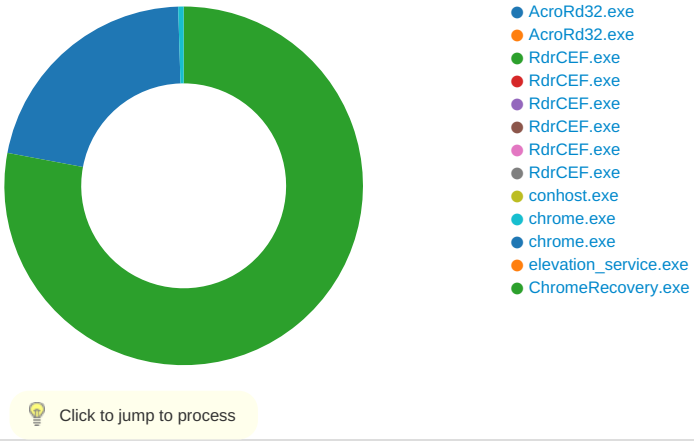
Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:07 UTC	197	OUT	GET / oPSIzNTIwdCIgaGVpZ2h0PSIzMjAiIHZpZXdCb3g9IjAgMCAzNTkgMjQwIj48ZGVmcz48Y2xpcFBhdGggaWQ9ImEiP jxwYXRoIGQ9Ik0xMjMgMGgyMzUuMzd2MjQwSDEyM3ptMCAwIi8+PC9jbGlwUGF0aD48L2RlZnM+PHBhdGggZD0iTTg 5LjY5IDU5LjEwMmg2Ny44MDJsLTEwLjUgNDAuMmMtMS42MDUgNS42LTQuNjA1IDEwLjEtOSAxMy41LTQ uNDAyIDMuNC05LjUwNCA1LjA5Ni0xNS4zIDUuMDk2aC0zMS41Yy03LjIgMC0xMy41LjEwMi0xOS4wNSA2LjMtN S41MDUgNC4yLTkuMzUzUzIDkuOTA0LTExLjU1MiAxNy4xMDMtMS40IDUuNDAzLTEuNTUgMTAuNS0uNDUgM TUuMzAyIDEuMDk4IDQuNzk2IDMuMDQ3IDkuMDUgNS44NTIgMTIuNzUgMi43OTcgMi43MDMgMi43OTcgMi43 5NyA4Ljg1IDQuMzk3IDIuMiA5LjE5OCAzLjI5OCAxNC40IDMuMjk4aDE5LjJjMy42MDIgMC4zNS0yLjQ1MyA4L jg1MiA0LjM1MiAyLjI5NyAyLjkwMiAyLjk0NSA2LjE0OCAxLjk1IDkuNzYsMS40NSAyLjk1NCAyLjQ1NCAyLjk wLTI3LjY1My0zLjE0OC0zOS43NS05LjQ1LTEyLjEwMi02Eplj48cGF0aCBkPSJNMTIzLjg5IDI0MEwxODIuO TkgMTguNjAyYzEuNTk4LTUuNTk4IDQuNTk4LTEwLjA5OCA5LTEzLjVDMTk2LjM4OCAxLjcgMTkuNjAyIDAgM yODggMGg2Mi43YzE0LjQwMyAwIDI3LjY1IDMuMTQ4IDM5Ljc1IDkuNDUgMTYuNzMgMTYuNjUgMzAuNSAzNS41 jU5NCAyNi45NTQtMS4yMDIgNDAuOTVsLTEuMiA0LjVjLTIuNTk3IDkuNjAyLTYuNTk3IDE4LjQ1LTEyIDI2LjU1LTU uMzk4IDguMDk4LTExLjg0NyAxNS4wNTItMTkuMzQzQ3IDIwLjg0OC03LjUgNS44NDUtMTUuODU1IDEwLjMwNSAyL jE4MS4zOTQtNC45OTcgMS41NDctOS45LjQ0NS0xNC43LTEuMS00LjgtMy4wNS05LjA0Ny01Ljg0OC0xMi43NS0yLjg tMy42OTUtNi40MDItNi42OTUtMTAuNzk2LTktNC40MDYtMi4yOTctOS4yMDYtMy40NS0xNC40MDItMy40NDUgMzMuM zlsLTQzLjggMTYyLjkwM2MtMS42MDYgNS40LTQuNjA2IDkuNzk3LTkgMTMuMTk1LTQuNDAzIDMuNDA3LTkuNDA2IDU uMTAyLTE1IDUuMTAyaC00MS43IiBmaWxsPSIjZmY2YzJiIi8+PC9nPjwvc3ZnPgo= HTTP/1.1 Host: webmail.unitedyacht.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183. 121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://arthurperush.com/css/cPanel.SharePoint_documentOnline/login.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-05-27 05:41:08 UTC	227	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 05:41:08 GMT Server: Apache/2.4.53 (cPanel) OpenSSL/1.1.1o mod_bwlimited/1.4 Content-Type: text/html; charset="utf-8" Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Cache-Control: no-cache, no-store, must-revalidate, private Content-Length: 40228 Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: webmailsession=%3aZNqgzC4382ir_xVC%2c3551e57f190c6a199ac67705514feaa1; HttpOnly; path=/; port=443; secure Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=webmail.unitedyacht.com; expires=Thu, 01-Jan-1970 00: 00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.unitedyacht.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; p ath=/; port=443; secure Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.unitedyacht.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde; port=443; secure Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: imp_key=expired; HttpOnly; domain=webmail.unitedyacht.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443; secure Set-Cookie: Horde=expired; HttpOnly; domain=.webmail.unitedyacht.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; p ath=/; port=443 Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.webmail.unitedyacht.com; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=443 Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Sat, 27-May-2023 05:41:08 GMT; path=/; port=443; secure Vary: Accept-Encoding,User-Agent Connection: close
2022-05-27 05:41:08 UTC	229	IN	Data Raw: 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 64 69 72 3d 22 6c 74 72 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f Data Ascii: <!DOCTYPE html><html lang="en" dir="ltr"><head> <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user- scalable=1"> <meta name="goo

Timestamp	kBytes transferred	Direction	Data
2022-05-27 05:41:08 UTC	235	IN	Data Raw: 79 4d 69 34 79 4e 54 51 67 4d 54 59 75 4e 53 41 7a 4e 53 34 31 4e 53 41 7a 49 44 45 7a 4c 6a 4d 77 4e 53 41 79 4c 6a 55 35 4e 43 41 79 4e 69 34 35 4e 54 51 74 4d 53 34 79 4d 44 49 67 4e 44 41 75 4f 54 56 73 4c 54 45 75 4d 69 41 30 4c 6a 56 6a 4c 54 49 75 4e 54 6b 33 49 44 6b 75 4e 6a 41 79 4c 54 59 75 4e 54 6b 33 49 44 45 34 4c 6a 51 31 4c 54 45 79 49 44 49 32 4c 6a 55 31 4c 54 55 75 4d 7a 6b 34 49 44 67 75 4d 44 6b 34 4c 54 45 78 4c 6a 67 30 4e 79 41 78 4e 53 34 77 4e 54 49 74 4d 54 6b 75 4d 7a 51 33 49 44 49 77 4c 6a 67 30 4f 43 30 33 4c 6a 55 67 4e 53 34 34 4d 44 55 74 4d 54 55 75 4f 44 55 31 49 44 45 77 4c 6a 4d 77 4e 53 30 79 4e 53 34 77 4e 53 41 78 4d 79 34 31 4c 54 6b 75 4d 69 41 7a 4c 6a 49 77 4e 43 30 78 4f 43 34 34 4d 44 55 67 4e 43 34 34 4d 44 Data Ascii: yMi4yNTQgMTYuNSAzNS41NSAzIDEzLjMwNSAyLjU5NCAyNi45NTQtMS4yMDIgNDAuOTVsLTEuMiA0LjVjLTIuNTk3IDkuNjAyLTYuNTk3IDE4LjQ1LTEyIDI2LjU1LTUuMzk4IDguMDk4LTExLjg0NyAxNS4wNTIttMTkuMzQ3IDIwLjg0OC03LjUgNS44NDUtMTUuODU1IDEwLjMwNS0yNS4wNSAxMy41LTkuMiAzLjIwNC0xOC44MDUgNC44MD

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: **4592**, Parent PID: **5700**

General

Target ID:	0
Start time:	07:39:15
Start date:	27/05/2022
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:\Users\user\Desktop\View Shared File.pdf
Imagebase:	0x870000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Registry Activities

Analysis Process: AcroRd32.exe PID: **5236**, Parent PID: **4592**

General	
Target ID:	1
Start time:	07:39:16
Start date:	27/05/2022
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" --type=renderer /prefetch:1 "C:\Users\user\Desktop\View Shared File.pdf
Imagebase:	0x870000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: **6240**, Parent PID: **4592**

General	
Target ID:	5
Start time:	07:39:22
Start date:	27/05/2022
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --backgroundcolor=16514043
Imagebase:	0xbd0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	3	CC59E2	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	26	CD83E5	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	104	CD8447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	220	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	8	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	24	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	8	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	success or wait	16	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	2176	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	60	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	12	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	7	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	2	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	success or wait	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	success or wait	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	4	CC59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	success or wait	8	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	success or wait	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	success or wait	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	success or wait	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	success or wait	24	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	success or wait	24	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	success or wait	56	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	success or wait	58	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	success or wait	1	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	2	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	success or wait	88	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	2	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	54	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	60	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	success or wait	20	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	19	CC59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	18	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	success or wait	19	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	239	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	285	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	success or wait	261	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	end of file	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	50	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	2	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	success or wait	195	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	end of file	2	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	25	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	success or wait	2	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	2	CC59E2	ReadFile
unknown	unknown	4096	success or wait	1	CC59E2	ReadFile
unknown	unknown	4096	end of file	1	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	success or wait	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	success or wait	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	success or wait	8	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	success or wait	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	end of file	3	CC59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	5	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	success or wait	2	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	2	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	10	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	success or wait	250	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	success or wait	12	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	success or wait	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	success or wait	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	success or wait	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	success or wait	24	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	success or wait	486	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	success or wait	1	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	success or wait	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	success or wait	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	success or wait	2	CC59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	success or wait	6	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	224	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	success or wait	18	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	success or wait	48	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	success or wait	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	success or wait	15	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	success or wait	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	success or wait	5	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	8	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	3	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css	unknown	4096	success or wait	1	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css	unknown	4096	end of file	1	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	success or wait	4	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	end of file	1	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js	unknown	4096	success or wait	1	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js	unknown	4096	end of file	1	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js	unknown	4096	success or wait	24	CC59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js	unknown	4096	end of file	1	CC59E2	ReadFile
\pipe\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	CD83E5	ReadFile

Analysis Process: RdrCEF.exe PID: **6416**, Parent PID: **6240**

General

Target ID:	6
Start time:	07:39:23
Start date:	27/05/2022
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1692,9505094711010095436,2813685380730867450,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=4522651327695846108 --lang=en-US --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=4522651327695846108 --renderer-client-id=2 --mojo-platform-channel-handle=1704 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xbd0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 6436, Parent PID: 6240

General

Target ID:	7
Start time:	07:39:23
Start date:	27/05/2022
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=gpu-process --field-trial-handle=1692,9505094711010095436,2813685380730867450,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --lang=en-US --gpu-preferences=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --service-request-channel-token=10689791772710628581 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job --ignored=" --type=renderer " /prefetch:2
Imagebase:	0xbd0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 6476, Parent PID: 6240

General

Target ID:	8
Start time:	07:39:24
Start date:	27/05/2022
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1692,9505094711010095436,2813685380730867450,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=1168505979000462944 --lang=en-US --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=1168505979000462944 --renderer-client-id=4 --mojo-platform-channel-handle=1812 --allow-no-sandbox-job /prefetch:1

Imagebase:	0xbd0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: **6588**, Parent PID: **6240**

General

Target ID:	9
Start time:	07:39:25
Start date:	27/05/2022
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1692,9505094711010095436,2813685380730867450,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=12017203034287935800 --lang=en-US --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=12017203034287935800 --renderer-client-id=5 --mojo-platform-channel-handle=2192 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xbd0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: **6168**, Parent PID: **6240**

General

Target ID:	18
Start time:	07:39:55
Start date:	27/05/2022
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe" --type=renderer --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --touch-events=enabled --field-trial-handle=1692,9505094711010095436,2813685380730867450,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=13253002013688982226 --lang=en-US --disable-pack-loading --log-file="C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --log-severity=disable --product-version="ReaderServices/19.12.20035 Chrome/80.0.0.0" --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=13253002013688982226 --renderer-client-id=6 --mojo-platform-channel-handle=2804 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xbd0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5200**, Parent PID: **6476**

General

Target ID:	29
Start time:	07:40:41
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: chrome.exe PID: **3152**, Parent PID: **4592**

General

Target ID:	34
Start time:	07:40:59
Start date:	27/05/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation -- "http://v2.bpkbsaya.com/wp-includes/css/cPanel.SharePoint_documentOnline/redirecting.php
Imagebase:	0x7ff7540f0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF7F62CFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: **7016**, Parent PID: **3152**

General

Target ID:	35
Start time:	07:41:01
Start date:	27/05/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1556,14589 80921024501746,2057635213361371639,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1908 /prefetch:8
Imagebase:	0x7ff7f6290000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: elevation_service.exe PID: **3876**, Parent PID: **568**

General

Target ID:	38
Start time:	07:42:25
Start date:	27/05/2022
Path:	C:\Program Files\Google\Chrome\Application\85.0.4183.121\elevation_service.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\85.0.4183.121\elevation_service.exe
Imagebase:	0x7ff75e9b0000
File size:	1322992 bytes
MD5 hash:	AFD137B53BA091ACBA569255B16DF837
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: ChromeRecovery.exe PID: **6240**, Parent PID: **3876**

General

Target ID:	39
Start time:	07:42:26
Start date:	27/05/2022
Path:	C:\Program Files\Google\Chrome\ChromeRecovery\scoped_dir3876_980132676\ChromeRecovery.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Google\Chrome\ChromeRecovery\scoped_dir3876_980132676\ChromeRecovery.exe" --appguid={8A69D345-D564-463c-AFF1-A69D9E530F96} --browser-version=85.0.4183.121 --sessionid={3300d716-561c-4453-9d4f-82432db65734} --system
Imagebase:	0x40000
File size:	259472 bytes
MD5 hash:	49AC3C96D270702A27B4895E4CE1F42A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly