

JoeSandbox Cloud BASIC



ID: 655755

Sample Name:

Invoice#0036473 .xlsx

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 16:27:35

Date: 01/07/2022

Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report Invoice#0036473 .xlsx	5
Overview	5
General Information	5
Detection	5
Signatures	5
Classification	5
Process Tree	5
Malware Configuration	5
Yara Signatures	5
Dropped Files	5
HTML	6
Sigma Signatures	6
Snort Signatures	6
Joe Sandbox Signatures	6
AV Detection	6
Phishing	6
Software Vulnerabilities	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	9
URLs	9
Domains and IPs	9
Contacted Domains	9
Contacted URLs	10
URLs from Memory and Binaries	10
World Map of Contacted IPs	13
Public IPs	13
Private	14
General Information	14
Warnings	14
Simulations	15
Behavior and APIs	15
Joe Sandbox View / Context	15
IPs	15
Domains	15
ASNs	15
JA3 Fingerprints	15
Dropped Files	15
Created / dropped Files	15
C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	15
C:\Users\user\AppData\Local\Google\Chrome\User Data\1aa1e2ae-a008-48f2-9a00-950f13de6f16.tmp	16
C:\Users\user\AppData\Local\Google\Chrome\User Data\25f44532-3c2e-40b6-b226-70d49123bf36.tmp	16
C:\Users\user\AppData\Local\Google\Chrome\User Data\426d4312-aea0-4881-af65-3e2d056b80e7.tmp	16
C:\Users\user\AppData\Local\Google\Chrome\User Data\645b6acd-32ef-46c5-b04e-45becdcbdc09.tmp	17
C:\Users\user\AppData\Local\Google\Chrome\User Data\7ba9cb53-984a-4699-8353-58f189a93a72.tmp	17
C:\Users\user\AppData\Local\Google\Chrome\User Data\81c675b7-7c7a-479c-ac72-9efc226a8ad9.tmp	17
C:\Users\user\AppData\Local\Google\Chrome\User Data\8a1a20b3-f5e6-4fe3-9a63-ad9192746343.tmp	18
C:\Users\user\AppData\Local\Google\Chrome\User Data\95b1abdd-d52f-4cbc-b086-3ae19d1e8029.tmp	18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	18
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2bb8be48-7e72-4290-bb6b-6ab5f3a98207.tmp	19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4071c3c0-9bab-4e09-96cb-097a690243fb.tmp	19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\71b843c2-4b70-4ce2-95c8-13f810853f15.tmp	19
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\85ab7ce1-3258-4e9b-a0e3-3e50db926871.tmp	20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\93422060-12de-434b-bf87-254d0ffca119.tmp	20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\962ced69-1c12-40da-8cbb-f3f48e7b42c7.tmp	20
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkgcccagldgiimedpiccmgmieda\1.0.0.6_0\metadata\computed_hashes.json	21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	21
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)	22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	22
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcapaombhbimeihdjneigic\def\6e83c16a-0f9f-4ba7-9421-b3a33db95024.tmp	23
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcapaombhbimeihdjneigic\def\GPUCache\data_1	23

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcphaaombhbimeihdjnejgic\def\Network Persistent State (copy)	24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\7e11f068-5877-44c9-9e16-a0421d08125b.tmp	24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	24
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State (copy)	25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c78cfa55-e1b4-4010-b1c1-a509d5123b73.tmp	25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d9b6f731-7f0c-4e5e-a34d-e1509d6c291d.tmp	25
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\dd213049-8a25-4006-9a0f-1b60de69be5e.tmp	26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\le087d5d6-61a6-4968-a1d6-b478e27ef5d7.tmp	26
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ff52ec09a-4950-4b99-81cc-a00db2867efe.tmp	27
C:\Users\user\AppData\Local\Google\Chrome\User Data\GrShaderCache\GPUCache\data_1	27
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	27
C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	28
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	28
C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)	28
C:\Users\user\AppData\Local\Google\Chrome\User Data\c31c0479-e4e4-4ded-825b-2ae50e1d6e8d.tmp	29
C:\Users\user\AppData\Local\Google\Chrome\User Data\le8b91c13-687e-4a5b-90e8-7c0373992032.tmp	29
C:\Users\user\AppData\Local\Google\Chrome\User Data\lec3a40c3-1400-4f01-815d-b48d30faaa73.tmp	29
C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\231C2286-1237-4321-A2E6-258BBA83D8CD	30
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Content.MSO\1A5C2F1B.tmp	30
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Content.MSO\FBE12F02.png	30
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\index[1].htm	31
C:\Users\user\AppData\Local\Temp\1828_1378596767_metadata\verified_contents.json	31
C:\Users\user\AppData\Local\Temp\1828_1378596767_platform_specific\x86_64\pnacl_public_pnacl.json	31
C:\Users\user\AppData\Local\Temp\1828_1378596767_platform_specific\x86_64\pnacl_public_x86_64.crtbegin_for_ah_o	32
C:\Users\user\AppData\Local\Temp\1828_1378596767_platform_specific\x86_64\pnacl_public_x86_64.crtbegin_o	32
C:\Users\user\AppData\Local\Temp\1828_1378596767_platform_specific\x86_64\pnacl_public_x86_64.crtend_o	32
C:\Users\user\AppData\Local\Temp\1828_1378596767_platform_specific\x86_64\pnacl_public_x86_64.ld_nexe	33
C:\Users\user\AppData\Local\Temp\1828_1378596767_platform_specific\x86_64\pnacl_public_x86_64.libcrt_platform_a	33
C:\Users\user\AppData\Local\Temp\1828_1378596767_platform_specific\x86_64\pnacl_public_x86_64.libgcc_a	33
C:\Users\user\AppData\Local\Temp\1828_1378596767_platform_specific\x86_64\pnacl_public_x86_64.libpnacl_irt_shim_a	34
C:\Users\user\AppData\Local\Temp\1828_1378596767_platform_specific\x86_64\pnacl_public_x86_64.libpnacl_irt_shim_dummy_a	34
C:\Users\user\AppData\Local\Temp\1828_1378596767_platform_specific\x86_64\pnacl_public_x86_64.pnacl_llc_nexe	34
C:\Users\user\AppData\Local\Temp\1828_1378596767_platform_specific\x86_64\pnacl_public_x86_64.pnacl_sz_nexe	35
C:\Users\user\AppData\Local\Temp\1828_1378596767\manifest.fingerprint	35
C:\Users\user\AppData\Local\Temp\1828_1378596767\manifest.json	35
C:\Users\user\AppData\Local\Temp\1828_877695470\Recovery.crx3	35
C:\Users\user\AppData\Local\Temp\1828_877695470_metadata\verified_contents.json	36
C:\Users\user\AppData\Local\Temp\1828_877695470\manifest.fingerprint	36
C:\Users\user\AppData\Local\Temp\1828_877695470\manifest.json	36
C:\Users\user\AppData\Local\Temp\3a6ddb19-0e1b-45fc-b970-e7ff4e6406ca.tmp	37
C:\Users\user\AppData\Local\Temp\cfba26a0-2d5f-46ad-b890-a1b6725a941d.tmp	37
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\bg\messages.json	37
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\ca\messages.json	38
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\cs\messages.json	38
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\da\messages.json	38
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\de\messages.json	38
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\el\messages.json	39
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\en\messages.json	39
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\en_GB\messages.json	39
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\es\messages.json	40
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\es_419\messages.json	40
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\et\messages.json	40
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\fi\messages.json	41
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\fil\messages.json	41
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\fr\messages.json	41
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\hi\messages.json	42
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\hr\messages.json	42
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\hu\messages.json	42
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\id\messages.json	42
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\it\messages.json	43
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\ja\messages.json	43
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\ko\messages.json	43
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\lt\messages.json	44
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\lv\messages.json	44
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\nb\messages.json	44
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\nl\messages.json	44
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\pl\messages.json	45
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\pt_BR\messages.json	45
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\pt_PT\messages.json	45
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\ro\messages.json	46
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\ru\messages.json	46
C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\sk\messages.json	46
Static File Info	47
General	47
File Icon	47

Network Behavior	47
Network Port Distribution	47
TCP Packets	47
UDP Packets	49
DNS Queries	50
DNS Answers	51
HTTP Request Dependency Graph	52
HTTPS Proxied Packets	52
Statistics	98
Behavior	98
System Behavior	98
Analysis Process: EXCEL.EXEPID: 6356, Parent PID: 756	98
General	98
File Activities	99
Registry Activities	99
Analysis Process: splwow64.exePID: 6548, Parent PID: 6356	99
General	99
File Activities	99
Analysis Process: chrome.exePID: 1828, Parent PID: 1468	99
General	99
File Activities	99
Registry Activities	99
Key Value Modified	100
Analysis Process: chrome.exePID: 4908, Parent PID: 1828	100
General	100
File Activities	100
Analysis Process: chrome.exePID: 6864, Parent PID: 6356	100
General	100
File Activities	101
Registry Activities	101
Analysis Process: chrome.exePID: 4944, Parent PID: 6864	101
General	101
Disassembly	101

Windows Analysis Report

Invoice#0036473 .xlsx

Overview

General Information

Sample Name:

Invoice#0036473 .xlsx

Analysis ID:

655755

MD5:

c93e6dcf32928e...

SHA1:

b90d66412b4d66.

SHA256:

3ffe69c9e2e2f8a..

Infos:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

HTMLPhisher

Score:

76

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Yara detected HtmlPhish10

Antivirus detection for URL or domain

Yara detected HtmlPhish7

Multi AV Scanner detection for dom...

Document exploit detected (process...

Found a high number of Window / U...

Potential document exploit detected...

No HTML title found

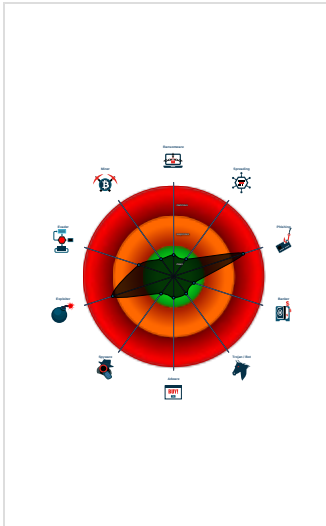
JA3 SSL client fingerprint seen in co...

Potential document exploit detected...

HTML body contains low number of ...

Potential document exploit detected...

Classification



Process Tree

System is w10x64

EXCELEXE (PID: 6356 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)

splwow64.exe (PID: 6548 cmdline: C:\Windows\splwow64.exe 12288 MD5: 8D59B31FF375059E3C32B17BF31A76D5)

chrome.exe (PID: 6864 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation -- "https://eyecandylashcompany.com/payment/frontend_paper_lantern/index.html MD5: C139654B5C1438A95B321BB01AD63EF6)

chrome.exe (PID: 4944 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1492,14547596045636120040,8967704105705094900,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1932 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)

chrome.exe (PID: 1828 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "https://eyecandylashcompany.com/payment/frontend_paper_lantern/index.html MD5: C139654B5C1438A95B321BB01AD63EF6)

chrome.exe (PID: 4908 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1572,2584016860965793630,9285400582768245070,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1916 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)

cleanup

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files				
Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\index[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\index[1].htm	JoeSecurity_HtmlPhish_7	Yara detected HtmlPhish_7	Joe Security	

Copyright Joe Security LLC 2022

Page 5 of 101

HTML				
Source	Rule	Description	Author	Strings
91064.0.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
91064.0.pages.csv	JoeSecurity_HtmlPhish_7	Yara detected HtmlPhish_7	Joe Security	

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

Multi AV Scanner detection for domain / URL

Phishing

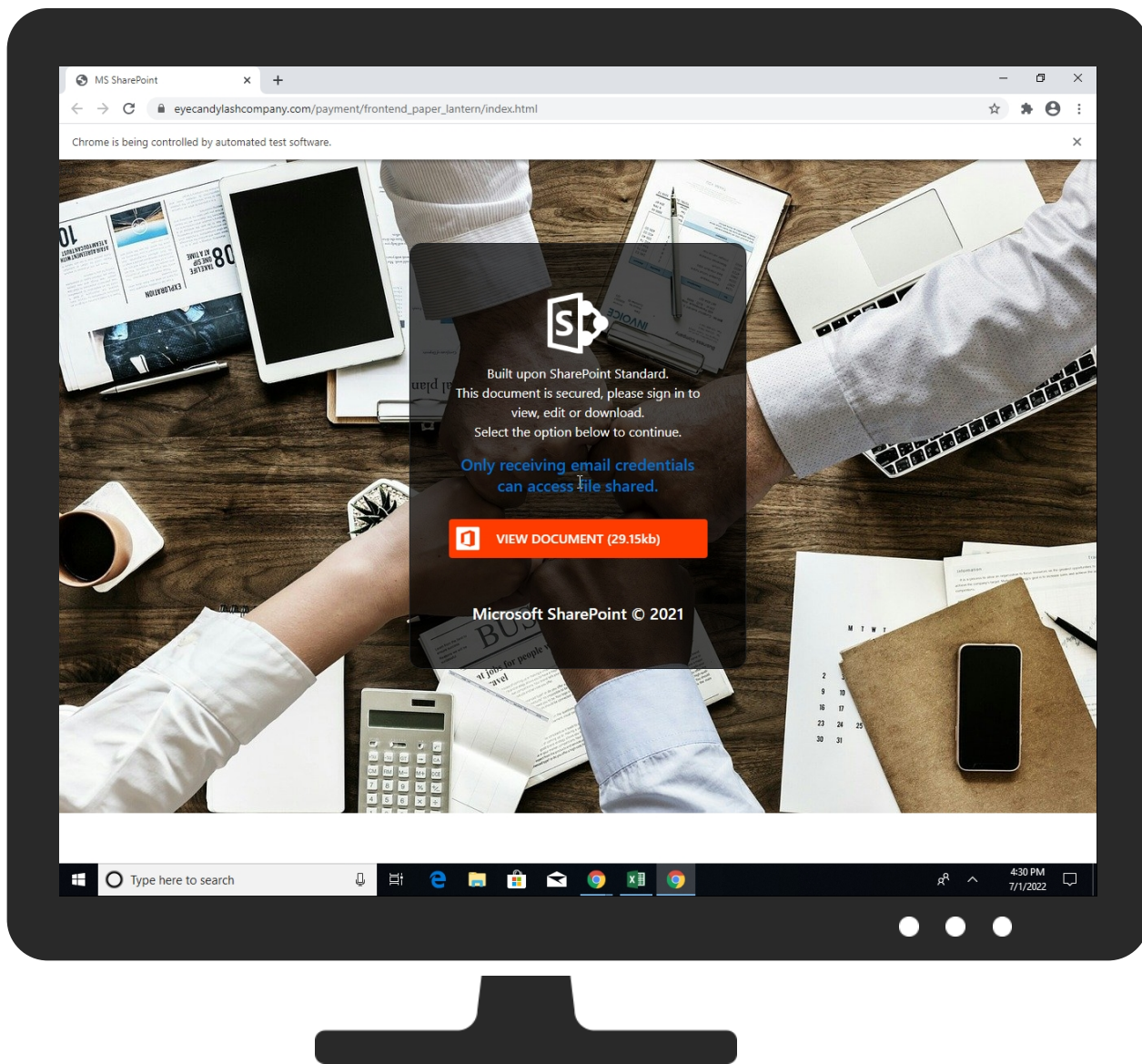
Yara detected HtmlPhish10

Yara detected HtmlPhish7

Software Vulnerabilities

Document exploit detected (process start blacklist hit)

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	 Exploitation for Client Execution	Path Interception	 Process Injection	 Masquerading	OS Credential Dumping	 Virtualization/Sandbox Evasion	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	 Extra Window Memory Injection	 Virtualization/Sandbox Evasion	LSASS Memory	 Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	 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)	 Process Injection	Security Account Manager	 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Invoice#0036473 .xlsx	5%	Virustotal		Browse
Invoice#0036473 .xlsx	8%	ReversingLabs	Document-Excel.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\1828_1378596767\platform_specific\x86_64\pnacl_public_x86_64_id_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1828_1378596767\platform_specific\x86_64\pnacl_public_x86_64_id_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1828_1378596767\platform_specific\x86_64\pnacl_public_x86_64_pnacl_iloc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1828_1378596767\platform_specific\x86_64\pnacl_public_x86_64_pnacl_iloc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1828_1378596767\platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1828_1378596767\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
eyecandylashcompany.com	6%	Virustotal		Browse

URLs				
Source	Detection	Scanner	Label	Link
http://https://eyecandylashcompany.com/payment/frontend_paper_lantern/index.html	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://eyecandylashcompany.com/payment/frontend_paper_lantern/images/office3651.png	100%	Avira URL Cloud	phishing	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://www.w3.or	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://eyecandylashcompany.com/payment/frontend_paper_lantern/images/gmail.png	100%	Avira URL Cloud	phishing	
http://www.w3.o	0%	URL Reputation	safe	
http://schemas.microsoft.cA.	0%	Avira URL Cloud	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://schemas.microsoft.	0%	URL Reputation	safe	
http://https://eyecandylashcompany.com/payment/frontend_paper_lantern/index.html2	100%	Avira URL Cloud	phishing	
http://https://wus2.pagecontentsync.	0%	URL Reputation	safe	
http://https://cortana.ai/api	0%	URL Reputation	safe	
http://schemas.mic	0%	URL Reputation	safe	
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	

Domains and IPs						
Contacted Domains						
Name	IP	Active	Malicious	Antivirus Detection	Reputation	
eyecandylashcompany.com	69.49.244.155	true	true	6%, Virustotal, Browse	unknown	
gstaticadssl.l.google.com	142.251.36.227	true	false		high	
stackpath.bootstrapcdn.com	104.18.10.207	true	false		high	
accounts.google.com	142.251.36.205	true	false		high	
cdnjs.cloudflare.com	104.17.24.14	true	false		high	
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high	
clients.l.google.com	142.251.36.238	true	false		high	
cdn.iconscout.com	104.18.28.243	true	false		high	
cdn.pixabay.com	172.64.150.12	true	false		high	
googlehosted.l.googleusercontent.com	172.217.16.161	true	false		high	
clients2.google.com	unknown	unknown	false		high	
ka-f.fontawesome.com	unknown	unknown	false		high	
code.jquery.com	unknown	unknown	false		high	
kit.fontawesome.com	unknown	unknown	false		high	
lh3.googleusercontent.com	unknown	unknown	false		high	

Contacted URLs			
Name	Malicious	Antivirus Detection	Reputation
http://https://eyecandylashcompany.com/payment/frontend_paper_lantern/images/office3651.png	true	Avira URL Cloud: phishing	unknown
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	false		high
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%3Dnmhkhkegcagldgiimedpiccmgmieda%26v%3D0.0.0.0%26install-edby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedckdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://eyecandylashcompany.com/payment/frontend_paper_lantern/images/gmail.png	true	Avira URL Cloud: phishing	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://eyecandylashcompany.com/payment/frontend_paper_lantern/index.html	true	SlashNext: Credential Stealing type: Phishing & Social Engineering	unknown
http://https://eyecandylashcompany.com/payment/frontend_paper_lantern/index.html	true	SlashNext: Credential Stealing type: Phishing & Social Engineering	unknown
http://https://cdn.pixabay.com/photo/2018/03/10/12/00/paper-3213924_1280.jpg	false		high

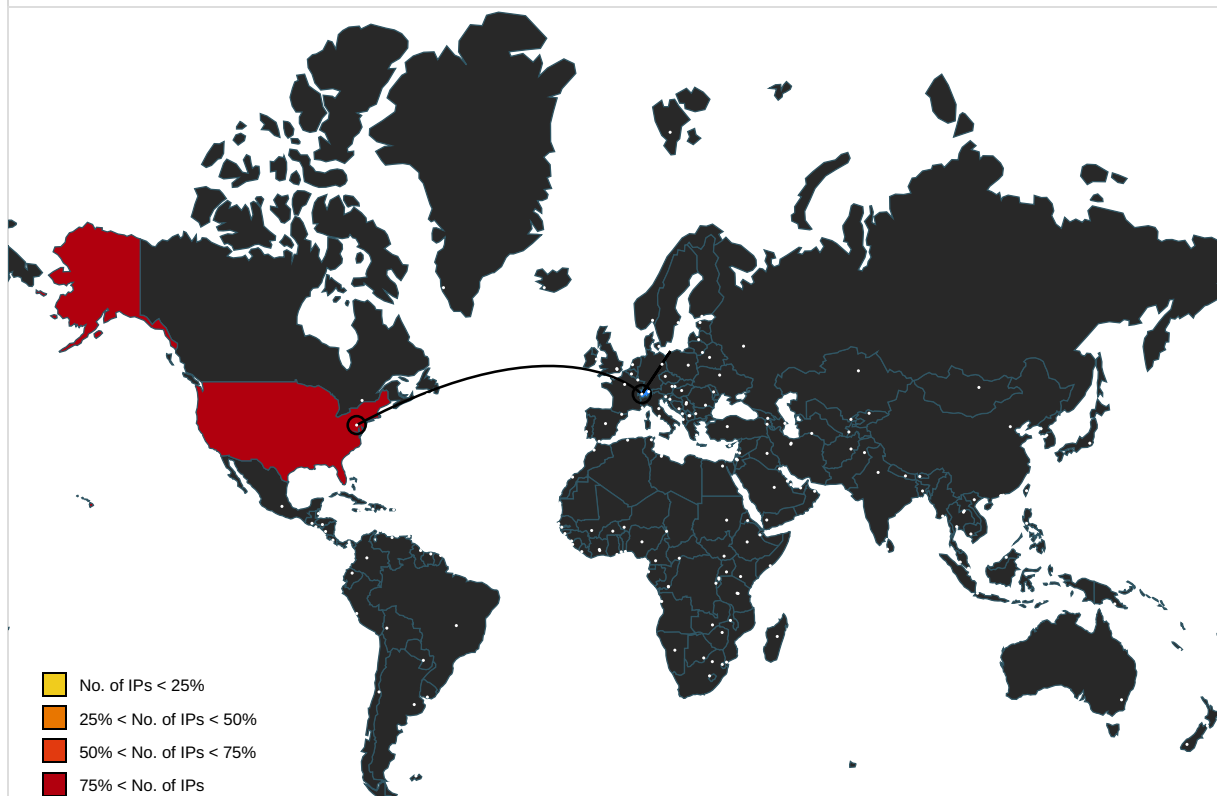
URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://shell.suite.office.com:1443	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://autodiscover-s.outlook.com/	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	index[1].htm.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://cdn.entity	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false	URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://rpssticket.partnerservices.getmicrosoftkey.com	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false	URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://api.aadrm.com/	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false	URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://api.microsoftstream.com/api/	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://cr.office.com	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://kit.fontawesome.com/585b051251.js	index[1].htm.0.dr	false		high
http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1	craw_window.js.19.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false	URL Reputation: safe	unknown
http://https://tasks.office.com	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	231C2286-1237-4321-A2E6-258BBA83D8CD.0.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.19.dr, craw_background.js.19.dr	false		high
http://https://store.office.cn/addinstemplate	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false	URL Reputation: safe	unknown
http://https://messaging.engagement.office.com/	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	craw_window.js.19.dr, manifest.json.19.dr	false		high
http://https://lh3.googleusercontent.com	71b843c2-4b70-4ce2-95c8-13f810853f15.tmp.20.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.w3.or	splwow64.exe, 00000001.00000003.276970217.0000000003A67000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 0000001.00000003.277087241.0000000003A6E000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.277056508.0000000003A6D000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false	URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://web.microsoftstream.com/video/	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false	URL Reputation: safe	unknown
http://https://graph.windows.net	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.19.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://ncus.contentsync.	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false	URL Reputation: safe	unknown
http://https://webdir.online.lync.com/autodiscover/autodiscover/service.svc/root/	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://weather.service.msn.com/data.aspx	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://wus2.contentsync.	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false	URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/ios	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://www.google.com/images/cleardot.gif	craw_window.js.19.dr	false		high
http://https://play.google.com	c78cfa55-e1b4-4010-b1c1-a509d5123b73.tmp.20.dr, 71b843c2-4b70-4ce2-95c8-13f810853f15.tmp.20.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/android/policies	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://entitlement.diagnostics.office.com	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://outlook.office.com/	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://accounts.google.com/MergeSession	craw_window.js.19.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://www.w3.o	splwow64.exe, 00000001.00000003.264411903.0000000002E95000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 0000001.00000003.264135446.0000000002E95000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.265089957.0000000002E95000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.264761149.0000000002E95000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://graph.windows.net/	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://apis.google.com	c78cfa55-e1b4-4010-b1c1-a509d5123b73.tmp.20.dr, 71b843c2-4b70-4ce2-95c8-13f810853f15.tmp.20.dr	false		high
http://https://devnull.onenote.com	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.microsoft.com .	splwow64.exe, 00000001.00000003.271415857.000000000FF8000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 0000001.00000003.271136883.000000000FF6000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.271110685.000000000FE7000.00000004.00000020.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://https://messaging.office.com/	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://skyapi.live.net/Activity/	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false	URL Reputation: safe	unknown
http://https://www.google.com/intl/en-US/chrome/blank.html	craw_background.js.19.dr	false		high
http://https://api.cortana.ai	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false	URL Reputation: safe	unknown
http://https://messaging.action.office.com/setcampaignaction	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://visio.uservoice.com/forums/368202-visio-on-devices	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://code.jquery.com/jquery-3.1.1.min.js	index[1].htm.0.dr	false		high
http://https://staging.cortana.ai	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false	URL Reputation: safe	unknown
http://https://onedrive.live.com/embed?	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://augloop.office.com	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://schemas.microsoft.	splwow64.exe, 00000001.00000003.283753202.000000002EAD000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 0000001.00000003.277683100.000000002EAD000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.272474325.000000002E95000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.272474325.000000002E95000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.278650127.000000002EAD000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.273927054.0000000003984000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.273448542.000000002EAD000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.273448542.000000002EAD000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.269980300.000000002EA3000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.287184725.000000000397D000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.273030293.000000002EAD000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.269103306.000000002EA3000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000002.639688445.000000002EAD000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.278038847.000000002EAD000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.269711890.000000002E9F000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.275038745.000000002EAD000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.286151322.000000002EAD000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.270225205.000000002EA6000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.269614889.000000002E95000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://chromium.googlesource.com/a/native_client/pnacl-llvm.git	pnacl_public_x86_64_libgcc_a.19.dr, pnacl_public_x86_64_pnacl_llvm_nexe.19.dr	false		high
http://https://api.diagnosticsdf.office.com/v2/file	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://code.jquery.com/jquery-3.3.1.js	index[1].htm.0.dr	false		high
http://https://prod.mds.office.com/mds/api/v1.0/clientmodeldirectory	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://api.diagnostics.office.com	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://store.office.de/addinstemplate	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://eyecandylashcompany.com/payment/frontend_paper_lantern/index.html2	History Provider Cache.19.dr	true	Avira URL Cloud: phishing	unknown
http://https://wus2.pagecontentsync.	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false	URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/datasets	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://cortana.ai/api	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false	URL Reputation: safe	unknown
http://https://clients2.googleusercontent.com	c78cfa55-e1b4-4010-b1c1-a509d5123b73.tmp.20.dr, 71b843c2-4b70-4ce2-95c8-13f810853f15.tmp.20.dr	false		high
http://https://chromium.googlesource.com/a/native_client/pnacl-clang.git	pnacl_public_x86_64_libgcc_a.19.dr, pnacl_public_x86_64_pnacl_llc_nexe.19.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json1.19.dr, manifest.json.19.dr	false		high
http://https://api.diagnosticsdf.office.com	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://login.microsoftonline.com/	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://schemas.mic	splwow64.exe, 00000001.00000003.274869798.0000000002E72000.00000004.00000020.00020000.00000000.sdmp, splwow64.exe, 00000001.00000003.277516468.0000000002E72000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://roaming.edog.	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false	URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false		high
http://https://powerlift.acompli.net	231C2286-1237-4321-A2E6-258BBA83D8CD.0.dr	false	URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.17.24.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.10.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
142.251.36.205	accounts.google.com	United States		15169	GOOGLEUS	false
142.251.36.238	clients.l.google.com	United States		15169	GOOGLEUS	false
142.251.36.227	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.18.28.243	cdn.iconscout.com	United States		13335	CLOUDFLARENETUS	false
172.64.150.12	cdn.pixabay.com	United States		13335	CLOUDFLARENETUS	false
69.49.244.155	eyecandylashcompany.com	United States		46606	UNIFIEDLAYER-AS-1US	true
172.217.16.161	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

Private
IP
192.168.2.1
127.0.0.1

General Information	
Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	655755
Start date and time: 01/07/202216:27:35	2022-07-01 16:27:35 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Invoice#0036473 .xlsx
Cookbook file name:	defaultwindowsofficecookbook.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
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	31
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:	mal76.phis.expl.winXLSX@38/128@18/12
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xlsx • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Browse link: https://eyecandylashcompany.com/payment/frontend_paper_lantern/index.html • Scroll down • Close Viewer

Warnings
• Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.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): 23.211.6.115, 52.109.76.141, 52.109.88.37, 52.109.76.34, 142.251.36.206, 142.251.36.195, 74.125.104.71, 34.104.35.123, 69.16.175.10, 69.16.175.42, 142.251.36.202, 142.251.37.10, 104.18.23.52, 104.18.22.52, 172.67.150.137, 104.21.30.41, 142.251.36.170
- Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, prod-w.nexus.live.com.akadns.net, ka-f.fontawesome.com.cdn.cloudflare.net, store-images.s-microsoft.com-c.edgekey.net, clientservices.googleapis.com, arc.msn.com, e12564.dspb.akamaiedge.net, redirector.gvt1.com, login.live.com, r2---sn-4g5lznlz.gvt1.com, sls.update.microsoft.com, update.googleapis.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com, www.bing.com, kit.fontawesome.com.cdn.cloudflare.net, fonts.googleapis.com, fs.microsoft.com, content-autofill.googleapis.com, ajax.googleapis.com, fonts.gstatic.com, prod.configsvc1.live.com.akadns.net, ris.api.iris.microsoft.com, r2.sn-4g5lznlz.gvt1.com, edgedl.me.gvt1.com, store-images.s-microsoft.com, config.officeapps.live.com, europe.configsvc1.live.com.akadns.net
- Not all processes were analyzed, report is 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
16:28:44	API Interceptor	1501x Sleep call for process: splwow64.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+FBIESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA

SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA8321101
Malicious:	false
Reputation:	high, very likely benign file
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 GNDXS.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 GM DS.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:\Users\user\AppData\Local\Google\Chrome\User Data\1aa1e2ae-a008-48f2-9a00-950f13de6f16.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.751587102034692
Encrypted:	false
SSDEEP:	384:hXJ2uwD5EjcyVb9CIN+r7vSa3BaE5HUhGFMrXkilxZU4srrTsmP030GGK1O8YGNX:pu2RpC0FdQeCiEOwYPn2aKsq2BT
MD5:	72B728383D83EB706C17FAAEAE8E82DC
SHA1:	2775E77E7128012329CFD0602A17EBB68B23750C
SHA-256:	29E842D2DAE2D4755E8938B2CD718DC5266FE0B700D3BDFC7DF07C60FFAA7378
SHA-512:	0714C990FE477FF8A87522E700DCEE9CFEE7404E610C1B5D15483A24BC362A83D4F09A2055413FDF1A3A14C8FFE3A9429DFF4BCB74418E8AB835A49EC158FE
Malicious:	false
Reputation:	low
Preview:	.q.....*...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.....`8.D...C::\P.r.o.g.r.a.m. .F.i.l.e.s\Co .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\25f44532-3c2e-40b6-b226-70d49123bf36.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.751518045797524
Encrypted:	false
SSDEEP:	384:RXJ2uwD5EjcyVb9CIN+r7vSa3BaE5HUhGFMrXkilxZU4srrTsmP7p30GGK1O8YGj:5u2RpC0MdQeCiEOwYPn2aKsq2Bh
MD5:	0F39597740F1422B557A339FCE17D215
SHA1:	6BBF35B7D73D67EB811BB66DBDD166A9646CD333
SHA-256:	9482079ECEFB987FEF7F9349AA54F3BF3CCF3871DA8BDC305739D9CDD9B29F0C
SHA-512:	99CA3569759E6981DE3FE095A70CD9AC7003C6542804F0AB6530570B9ACF919EFCDB2C800BB71153B2712995B62DBA4D9C921FF0DB72FA9B946ACE648A00A5
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.....`8.D...C::\P.r.o.g.r.a.m. .F.i.l.e.s\Co .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\426d4312-aea0-4881-af65-3e2d056b80e7.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):	205858
Entropy (8bit):	6.043125146569017
Encrypted:	false
SSDEEP:	6144:kogQRUdqIM7dKoOO2Z9gK1YcUaqfIIUOoSiuRL:kNDdqE70oOI9gKVzo8
MD5:	B7A07F14C072DC7758BEAEEC84EC6A43

SHA1:	386C1B1A0AAD94288BD14D56DB015684151CB99B
SHA-256:	B79AB9F195C44D21E7CDC3FA5ABB843A03498F1E1663CA063E7B91556C447531
SHA-512:	62E67BB2DD8ECBAF01B87822C06845DE5CB06B367161026442F7EB715737ABE03FB27C7C632B8EFD5B9F2DCF8756055F7BC25A8233AD3F600437FC16D6E98E6B
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": "1.6567181986874e+12", "network": "1.6566858e+12", "ticks": "195698446.0", "uncertainty": "3745423.0" }, "os_crypt": { "encrypted_key": "RFBBUeKBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WK194zTZq03WydZHLcAAAAAIAAAAAABBmAAAAQAIAAAABAL2tyan+IsWtxhoUVdUYrYiwg8iJkppNr2ZbFie9UAAAAA6AAAAAaAIAAAABDv4gjLq1dOS7lKRG21YVXojnHhsRhNbP8/D1zs78mXMAAAB045Od5v4BxiFP4bdRYjJDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdflljw4oXIE4R7I0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGwCOPFyXOajfBL3GXBUhMXghJbDGB5WCu+JEdxaxLLxaYPp4zeP", "password_manager": { "os_password_blank": true, "os_password_last_changed": "13291230639357535", "plugins": { "metadata": { "adobe-flash-player": { "display

C:\Users\user\AppData\Local\Google\Chrome\User Data\645b6acd-32ef-46c5-b04e-45becdcdbc09.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):	214207
Entropy (8bit):	6.0707986108681595
Encrypted:	false
SSDEEP:	6144:PJogQRUdqIM7dKoOO2Z9gK1YcUaqfIUOoSiuRL:PJNDdqe70oOI9gKVzo8
MD5:	BE10E6D77F4BEE264FA8F6719787C6CD
SHA1:	F2CFD881AC15102BB3356BF5881C7C4A1A3F16DC
SHA-256:	8F6D3DDFF45F2D25D57124B65C367840DA5ADB0D38678E46087088D4C4106C1E
SHA-512:	5F61517F9B589F91332F8E2D692724F618A4C0039B2186B5DD4A6F55176659FBBBD3395081BC4D243C5357FFF050CC024256864BAC3464AE55CC9B0FEB29FA2
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": "1.6567181986874e+12", "network": "1.6566858e+12", "ticks": "195698446.0", "uncertainty": "3745423.0" }, "os_crypt": { "encrypted_key": "RFBBUeKBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WK194zTZq03WydZHLcAAAAAIAAAAAABBmAAAAQAIAAAABAL2tyan+IsWtxhoUVdUYrYiwg8iJkppNr2ZbFie9UAAAAA6AAAAAaAIAAAABDv4gjLq1dOS7lKRG21YVXojnHhsRhNbP8/D1zs78mXMAAAB045Od5v4BxiFP4bdRYjJDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdflljw4oXIE4R7I0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGwCOPFyXOajfBL3GXBUhMXghJbDGB5WCu+JEdxaxLLxaYPp4zeP", "password_manager": { "os_password_blank": true, "os_password_last_changed": "13291230639357535", "plugins": { "metadata": { "adobe-flash-player": { "display

C:\Users\user\AppData\Local\Google\Chrome\User Data\7ba9cb53-984a-4699-8353-58f189a93a72.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):	214207
Entropy (8bit):	6.070798103289104
Encrypted:	false
SSDEEP:	6144:fUogQRUdqIM7dKoOO2Z9gK1YcUaqfIUOoSiuRL:fUNDdqe70oOI9gKVzo8
MD5:	5E33186D842CF2A9E81078910FEBB39F
SHA1:	B8396FF238687BF724D1E53332BDA7D26F8A6630
SHA-256:	3BA4D6A5AD9706F7D1DE9F67B7C5E4A2B0458AFAA44671392F817B3C4156290B
SHA-512:	BB0F82166360E2938E8D62D91EE5497D4A612C1D8A804A423D377A6AB7A78EAD4FEEFCFAFEA0259F5A1F4578A0A116F2816B775F126E9B1494CC0D459ED7EF1B3
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": "1.6567181986874e+12", "network": "1.6566858e+12", "ticks": "195698446.0", "uncertainty": "3745423.0" }, "os_crypt": { "encrypted_key": "RFBBUeKBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WK194zTZq03WydZHLcAAAAAIAAAAAABBmAAAAQAIAAAABAL2tyan+IsWtxhoUVdUYrYiwg8iJkppNr2ZbFie9UAAAAA6AAAAAaAIAAAABDv4gjLq1dOS7lKRG21YVXojnHhsRhNbP8/D1zs78mXMAAAB045Od5v4BxiFP4bdRYjJDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdflljw4oXIE4R7I0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGwCOPFyXOajfBL3GXBUhMXghJbDGB5WCu+JEdxaxLLxaYPp4zeP", "password_manager": { "os_password_blank": true, "os_password_last_changed": "13245951016607996", "plugins": { "metadata": { "adobe-flash-player": { "display

C:\Users\user\AppData\Local\Google\Chrome\User Data\81c675b7-7c7a-479c-ac72-9efc226a8ad9.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):	214207
Entropy (8bit):	6.070798103289104
Encrypted:	false
SSDEEP:	6144:fUogQRUdqIM7dKoOO2Z9gK1YcUaqfIUOoSiuRL:fUNDdqe70oOI9gKVzo8
MD5:	5E33186D842CF2A9E81078910FEBB39F

SHA1:	B8396FF238687BF724D1E5332BDA7D26F8A6630
SHA-256:	3BA4D6A5AD9706F7D1DE9F67B7C5E4A2B0458FAA44671392F817B3C4156290B
SHA-512:	BB0F82166360E2938E8D62D91EE5497D4A612C1D8A804A423D377A6AB7A78EAD4FEEFCAFEA0259F5A1F4578A0A116F2816B775F126E9B1494CC0D459ED7EF1B3
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": "1.6567181986874e+12", "network": "1.6566858e+12", "ticks": "195698446.0", "uncertainty": "3745423.0" }, "os_crypt": { "encrypted_key": "RFBBUeKBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydZHLcAAAAAIAAAAAABBmAAAAQAAlAAABAL2tyan+IsWtxhoUVdUYrYiwg8iKppNr2ZbBFie9UAAAAA6AAAAAaAIAAAABDv4gjLq1dOS7lKRG21YVXojnHhsRhNbP8/D1zs78mXMAAAB045Od5v4BxiFP4bdRYjJDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfjw4oXIE4R7I0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGB5WCu+JEdxaxLLxaYPp4zeP", "password_manager": { "os_password_blank": true, "os_password_last_changed": "13245951016607996", "plugins": { "metadata": { "adobe-flash-player": { "display

C:\Users\user\AppData\Local\Google\Chrome\User Data\8a1a20b3-f5e6-4fe3-9a63-ad9192746343.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):	214206
Entropy (8bit):	6.07079771071813
Encrypted:	false
SSDEEP:	6144:GQogQRUdqlM7dKoOO2Z9gK1YcNaqfilUOoSiuRL:GQNDdqe70oOl9gKVuo8
MD5:	DBC2001EFF8231AEC5FB53BEAB02A779
SHA1:	3CE65CD86017A3377A77B3D7BD81B19A1223BBE5
SHA-256:	9CECF660C23285CDB9862E8280198BD78733A98806B7529E667C586098F701BB
SHA-512:	474AB58E05FD68E8831579FC9F3DEACC042B34A277AB322EBAD561436A6F3FFCC8BF421D678A2D9E61A59C2B35EA10A900231F9BADA7030B309558E1FE28C6C4
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": "1.6567181986874e+12", "network": "1.6566858e+12", "ticks": "195698446.0", "uncertainty": "3745423.0" }, "os_crypt": { "encrypted_key": "RFBBUeKBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydZHLcAAAAAIAAAAAABBmAAAAQAAlAAABAL2tyan+IsWtxhoUVdUYrYiwg8iKppNr2ZbBFie9UAAAAA6AAAAAaAIAAAABDv4gjLq1dOS7lKRG21YVXojnHhsRhNbP8/D1zs78mXMAAAB045Od5v4BxiFP4bdRYjJDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfjw4oXIE4R7I0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGB5WCu+JEdxaxLLxaYPp4zeP", "password_manager": { "os_password_blank": true, "os_password_last_changed": "13245951016607996", "plugins": { "metadata": { "adobe-flash-player": { "display

C:\Users\user\AppData\Local\Google\Chrome\User Data\95b1abdd-d52f-4cbc-b086-3ae19d1e8029.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.751387873266962
Encrypted:	false
SSDEEP:	384:nXJ2uwD54c7CIN+r7vSa3BaE5HUhGFMrXkilzU4srrTSmP030GGK1O8YGNX12fV;j2RpC0FdQeCiEOwYPn2aKsq2BW
MD5:	0CE7A67BB83EBE0F38E71DCFC79D80AA
SHA1:	95C69A25B58293F90603AC638F8CBA334795F1A6
SHA-256:	00F19F05106AC9511F96E349B49A5AEF1C4B54101C0A104692CDCA445C59D992
SHA-512:	067D76E92A4F5AFB91AE23177D8427398B6178AE815C9145BD919772EB71742A0D0ED897E45F5EE09874503ECC7E09A288DA9590B42F611CB5FB7BAB0C2AF6CF
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..Pl...])...%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.....'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\2bb8be48-7e72-4290-bb6b-6ab5f3a98207.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCDBD92598A0F13D313CC9EBC2A07E61F007BAF58FBFB94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4071c3c0-9bab-4e09-96cb-097a690243fb.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):	17702
Entropy (8bit):	5.577273801702975
Encrypted:	false
SSDEEP:	384:ZfGt1LLuWXR1kXqKf/pUZNCgVLH2HfD7rUeG29Q24p:GLl/R1kXqKf/pUZNCgVLH2Hf/rUel2K
MD5:	96CF31ECE2DAE0E80667A04FC2A2AFF3
SHA1:	F83776469763D07A04A595F803253ABAEAC4DE75
SHA-256:	3B6F51CF3543B00F2AD3D4E047286FC51338176B959BA6CE4B58FDCEBAE881F3
SHA-512:	CA4DBE0AF8D7A1481D94BBA97C38C44DD6EAEBD4E437E72C5FBDC1127177DC6DE01A1C1283980EF4ECAEA73926172BA7D5265B992F03D4F824D15072A287737
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf:doc:docx:docm:xls:xlsx:xlsm:xlsx:ppt:pptx:pptm:mhtml:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwp: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":"13301191796298773","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\71b843c2-4b70-4ce2-95c8-13f810853f15.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):	2533
Entropy (8bit):	4.899174475228989
Encrypted:	false
SSDEEP:	48:Y2TntwXGDH3qyvz5s8GskRLsVqasIMHisO2RsGO7sy5s9bNbD:JTnOXGDHa+zX216GlpOXypH
MD5:	1046D0992E1A3D2F0A9342F2B885C5F1
SHA1:	336AF2595C3A1A2049B3077CCA4F4695E633FB10
SHA-256:	FC98C5E38D326B256DAED47655114B69D5EC08298181D5A366B7DC98B974D90F
SHA-512:	3424CE859BD357FEDE67CD82425054A998F42027C0401809E57D4448C2EAF0FE39E16F9A483DA181B517365FDD280EDD7650C05E868516DDB61ADE93F39DBBF1A
Malicious:	false

Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":"pdf.doc:docx:docxm:docm:xls:xlsx:xlsm:xlsm:ppt:pptx:pptxm:pptm:mht:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsb:xll:hwp:show:cell:hwp:x: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":"13301191796298773","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\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:GbylJnlTwGB7V9Hne4qasKxXltnLG48gcLg/Pkl:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9C8BCFD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bTPkyBxp3hN2slpI0=","WSOpQRkYTHjPSIG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6Rl=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtlGsCefvuceTpAatmLvul11RJJA=","dHjvMSlIdjj7MWGg3T8MG58RuugRXk32vqi/13JqEgA=","zD3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTi=","DpjXcO85FFFY9KJFPkGNfUtdQlOsgwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofl9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGObGOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOStHVFwN8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1lJdn/UtbNAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxE+wG3QJmuYWEvYCs40NI=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWvhPNxJXO1C/n68=","E3vWWLQxznmj+e5QxYbUscIJ5n0lTpW5JBHV1Kph3/KM=","i3l8ghdTf9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSILPhrtuOhGyrHn3llsMHqBbi70gkljEE=","rhIzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","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):	369
Entropy (8bit):	5.228210359116467
Encrypted:	false
SSDEEP:	6:63/1VbF7q2PWXp+N23iKKdK25+Xqx8chl+IFUtqV53/1VxZmwYV53/1VdFOFkwOx:alF7va5KkTXfchl3FUtsb/CoF5f5KkTM
MD5:	D8786D507C4C02FDB7E875D0D8D1C2E8
SHA1:	63BACB39E7559F61BA8576CA60ECE22EB31D389
SHA-256:	90D94AAE581B7A269BD42901E318807A694B7CE34FFCCC15ABA461110FDCB3A1
SHA-512:	31B4AB31A895EFC473DFBA2E62BF82E8BDAF01A2BED34C5F89A8D2655ED26EE6651D6E0A8D7E12EE8DE6678AC1D12F2C5FDA96C1E012813A9F2D3C8EA58CBE46
Malicious:	false
Preview:	2022/07/01-16:30:04.732 160 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\MANIFEST-000001.2022/07/01-16:30:04.733 160 Recovering log #3.2022/07/01-16:30:04.734 160 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):	369
Entropy (8bit):	5.228210359116467
Encrypted:	false
SSDEEP:	6:63/1VbF7q2PWXp+N23iKKdK25+Xqx8chl+IFUtqV53/1VxZmwYV53/1VdFOFkwOx:alF7va5KkTXfchl3FUtsb/CoF5f5KkTM
MD5:	D8786D507C4C02FDB7E875D0D8D1C2E8
SHA1:	63BACB39E7559F61BA8576CA60ECE222EB31D389
SHA-256:	90D94AAE581B7A269BD42901E318807A694B7CE34FFCCC15ABA461110FDCB3A1
SHA-512:	31B4AB31A895EFC473DFBA2E62BF82E8BDAF01A2BED34C5F89A8D2655ED26EE6651D6E0A8D7E12EE8DE6678AC1D12F2C5FDA96C1E012813A9F2D3C8EA58CBE46
Malicious:	false
Preview:	2022/07/01-16:30:04.732 160 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\MANIFEST-000001.2022/07/01-16:30:04.733 160 Recovering log #3.2022/07/01-16:30:04.734 160 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):	719
Entropy (8bit):	5.270212628974301
Encrypted:	false
SSDEEP:	12:58nbyXbB+EyaSlvAgQh7BVJ1aX37Wfkyofn1C1TBk778B/xgskZBa9sNiyVudiy9:5m2CabvAzdja7Cyfn16Y78BJgskfa9yq
MD5:	619881096EFE39459BD2A4B9EB2E346B
SHA1:	89331730D2D27387E9CA4EE64045C9503B1F5C41
SHA-256:	3F2651738D0344A6054D3A187F33F1DCE461BFD6540CE3CEE8880F33263A5354
SHA-512:	D03DDB1EA80127C21DD7F08D964EFD5EDEF5CB64BC958A7DA8E66A91481ABD91715C77E24AB2EF71A2E08A4908D163043C2B65871167BE37F264B036BA3F0A6C
Malicious:	false
Preview:	"c....com..eyecandylashcompany..frontend..html..https..index..lantern..ms.....paper..payment..sharepoint*.....com.....eyecandylashcompany.....frontend.....html.....https.....index.....lantern.....ms.....paper.....payment.....sharepoint..2.....a.....c.....d.....e.....f.....h.....i.....l.....m.....n.....o.....p.....r.....s.....t.....u.....v.....w.....x.....y.....z.....e.....*https://eyecandylashcompany.com/payment/frontend_paper_lantern/index.html2.MS SharePoint:.....J..... (17?E....

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):	2533
Entropy (8bit):	4.899174475228989
Encrypted:	false
SSDEEP:	48:Y2TntwXGDH3qyvz5s8GskRLsVqasIMHisO2RsGO7sy5s9bNbD:JTnOXGDHa+zX216GlpOXypH
MD5:	1046D0992E1A3D2F0A9342F2B885C5F1
SHA1:	336AF2595C3A1A2049B3077CCA4F4695E633FB10
SHA-256:	FC98C5E38D326B256DAED74655114B69D5EC08298181D5A366B7DC98B974D90F
SHA-512:	3424CE859BD357FEDE67CD82425054A998F42027C0401809E57D4448C2EAF0FE39E16F9A483DA181B517365FDD280EDD7650C05E868516DDB61ADE93F39DBBFA
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://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": "13303783799969491", "port": 443, "protocol_str": "quic" }, "isolation": [], "server": "https://redirector.gvt1.com" }, { "alternative_service": { "advertised_versions": [50], "expiration": "13303783799993249", "port": 443, "protocol_str": "

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

[illegible]

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):	5.564183009590256
Encrypted:	false
SSDEEP:	384:ZfGtcLuWXR1kXqKf/pUZNCgVLH2HfD7rU9HGszZ29x24Lc:RL/R1kXqKf/pUZNCgVLH2Hf/rUhGsMG
MD5:	4427796AA7B0E6AD24B2D6B1BC4D2637
SHA1:	DB732DA467256833BC1A8748A9096BC732D78602
SHA-256:	AB19662ED6FE9454193670744B7CD6A37A1F6ADFFE239C5C43B9A89CBA9E922B
SHA-512:	F5AB7EDDB18AE2E2BF919037F81CC8BB22789DD46C04A5DCDDCC05A4AD022FB0BF1F1903F6AAD38D559C9522C54B9A65249D1D5D7BAC3E7293BC16201BDDCCB6
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":,"pdf.doc:docx:docm:xls:xlsx:xlsm:xlsm:ppt:pptx:pptxm:pptm:mhtml:rtf:pub:vsd:mpp:mdb:dot:dotm:xlsm:xl:hwpx:show:cell:hwpx:hwt:jtd:zip:iso:7z:rar:tar:vbs:js:jse:vbe:exe:html:htm:xhtml:tbz2:lz","extensions":{"settings":{"ahfgeienlihckogmohjhadlkgjocpleb":{"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":"13301191796298773","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\6e83c16a-0f9f-4ba7-9421-b3a33db95024.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:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB43BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Preview:	{\"net\":{\"http_server_properties\":{\"servers\":{\"alternative_service\":{\"advertised_versions\":{\"[50],\"expiration\":\"13248543490879170\",\"port\":443,\"protocol_str\":\"quic\"},{\"advised_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\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:MsEIIllkEthXllkl2zE:/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):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BB005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
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":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmhkhkegccagldgiimedpiccmgmieda\def\7e11f068-5877-44c9-9e16-a0421d08125b.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):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/fy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071B1
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":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmhkhkegccagldgiimedpiccmgmieda\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:MsEIIllkEthXllkl2zE:/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):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/fy
MD5:	F4FEFEEEC727272F9DC0FCE1B52D79B5
SHA1:	00EECF3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071B1
Malicious:	false
Preview:	{ "net": { "http_server_properties": { "servers": { { "alternative_service": { { "advertised_versions": [50], "expiration": "13248543498399332", "port": 443, "protocol_str": "quic" }, { "adve rtised_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": "4G" } } }

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c78cfa55-e1b4-4010-b1c1-a509d5123b73.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/soBDysKqnsIzMhPDClsWJMHLSNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4AAE22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC48472F27F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD160:
Malicious:	false
Preview:	{ "net": { "http_server_properties": { "servers": { { "alternative_service": { { "advertised_versions": [], "expiration": "13248543677350473", "port": 443, "protocol_str": "quic" }, { "advert ised_versions": [], "expiration": "13248543677350474", "port": 443, "protocol_str": "quic" }, "isolation": [], "network_stats": { "srtt": 31344 }, "server": "https://dns.google", "support s_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": "1324854350 1454994", "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\d9b6f731-7f0c-4e5e-a34d-e1509d6c291d.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):	5218
Entropy (8bit):	4.986633380855184
Encrypted:	false
SSDEEP:	96:nyC4mt1pcKIsok0JCKL8a6Wk0gEtqbOTQVuw:nnyCR1pcR4K1k9r
MD5:	D4CE804FF050AB17A26F6E3E9DE36066
SHA1:	DC7578848BB025CD5F24925472F32C3601EF010
SHA-256:	0FC57567349801E620386E69E2215C41100AD83E506A6676CFBE48BF2E0A21F0
SHA-512:	DCD0B25B0BD2C8AEEEF6D24A853C62595BFE8B8630EB20DC980F874CF3E4FB4CE5D1CD1B197B3B3312386E9FDE0C84BC63D7E33BF144D4A78ADD3C790FE68ABA
Malicious:	false

[illegible]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f52ec09a-4950-4b99-81cc-a00db2867efe.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):	5.564183009590256
Encrypted:	false
SSDEEP:	384:ZfGtclUWXR1kXqKf/pUZNCgVLH2HFd7rU9HGzS29x24Lc:RL/R1kXqKf/pUZNCgVLH2HF/rUhGsMG
MD5:	4427796AA7B0E6AD24B2D6B1BC4D2637
SHA1:	DB732DA467256833BC1A8748A9096BC732D78602
SHA-256:	AB19662ED6FE9454193670744B7CD6A37A1F6ADFEE239C5C43B9A89CBA9E922B
SHA-512:	F5AB7EDDB18AE2E2BF919037F81CC8B8B22789DD46C0A45DCDDCC05A4AD022FB0BF1F1903F6AAD38D559C9522C54B9A65249D1D5D7BAC3E7293BC16201BD CCB6
Malicious:	false
Preview:	{"download":{"always_open_pdf_externally":true,"directory_upgrade":true,"extensions_to_open":".pdf.doc.docx.docm.xls.xlsx.xlsm.xlsm.ppt.pptx.pptxm.pptm.mht.rtf.pub.vsd.mpp.mdb.dot.dotm.xlsb.xml.hwp.show.cell.hwp.xhwt.jtd.zip.iso.7z.rar.tar.vbs.js.jse.vbe.exe.html.htm.xhtml.tbz2.lz"},"extensions":{"setings":{"ahfgeienlihck ogmohjhaddlkjgocpleb":{"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":"13301191796298773","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\GrShaderCache\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0018238520723782249
Encrypted:	false
SSDEEP:	3:MsElIlIkEthXIlkl2zELqCjtl:/M/xT02zSBI
MD5:	4D6A87B837034502A12B3821F7C67DB9
SHA1:	2D9AEFD5997E23FA1AC4FCD4F3BEF29FB8514207
SHA-256:	774273543D373714C0F766A844038E50D14A69C70281883599D0EF65F7E10D92
SHA-512:	599B9EF531293B6AE2D99E2F105E0A5ECE1AD8CF998FD0F14B812A62080527B0AC4BB67970E761D05B6CB5C1ED5AC3D313E05812E7BEF20AFD1FAC7394B797D8
Malicious:	false
Preview:	

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:tbloIlrJ5ldQxl7aXVdJiG6R0RIAl:tbdlrnQxZaHIGiOR6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEBF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
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:	86010ED2B2EEBDC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
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):	214206
Entropy (8bit):	6.07079771071813
Encrypted:	false
SSDEEP:	6144:GQogQRUdqIM7dKoOOZ29gK1YcNaqfllUOoSiuRL:GQNDdqe70oOI9gKvUo8
MD5:	DBC2001EFF8231AEC5FB53BEAB02A779
SHA1:	3CE65CD86017A3377A77B3D7BD81B19A1223BBE5
SHA-256:	9CECF660C23285CDB9862E8280198BD78733A98806B7529E667C586098F701BB
SHA-512:	474AB58E05FD68E8831579FC9F3DEACC042B34A277AB322EBAD561436A6F3FFCC8BF421D678A2D9E61A59C2B35EA10A900231F9BADA7030B309558E1FE28C6C4
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\":\"1.6567181986874e+12\",\"network\":\"1.6566858e+12\",\"ticks\":\"195698446.0\",\"uncertainty\":3745423.0}},\"os_crypt\":{\"encrypted_key\":\"RFBUEkBAAAA0lyd3wEV0RGMEgDAT8KX6wEAAABL95WKI94zTZq03WydZHLcAAAAAIAAAAAABBmAAAAQAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbFie9UAAAAA6AAAAAagAAIAAAABDv4gjlQ1dOS7IkRG21YVXojnHsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7I0AAAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGB5WCu+JEdxaxLLxaYPp4zeP\"},\"password_manager\":{\"os_password_blank\":true,\"os_password_last_changed\":\"13245951016607996\"},\"plugins\":{\"metadata\":{\"adobe-flash-player\":{\"displayu

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):	95428
Entropy (8bit):	3.751518045797524
Encrypted:	false
SSDEEP:	384:RXJ2uwD5EjcyVb9CIN+r7vSa3BaE5HUhGFMrXkilxZU4srrTsmP7p30GGK1O8YGj:5u2RpC0MdQeCiEOwYPn2aKsq2Bh
MD5:	0F39597740F1422B557A339FCE17D215
SHA1:	6BBF35B7D73D67EB811B666DBDD166A964CD333
SHA-256:	9482079CECFB987FEF7F9349AA54F3BF3CCF3871DA8BDC305739D9CDD9B29F0C
SHA-512:	99CA3569759E6981DE3FE095A70CD9AC7003C6542804F0AB6530570B9ACF919EFCDB2C800BB71153B2712995B62DBA4D9C921FF0BD72FA9B946ACE648A00A5

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.....8D...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\c31c0479-e4e4-4ded-825b-2ae50e1d6e8d.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):	205766
Entropy (8bit):	6.042879285454642
Encrypted:	false
SSDEEP:	6144:gogQRUdqIM7dKoOO2Z9gK1YcUaqfIUoOsiuRL:gNDdqe70oOI9gKVzo8
MD5:	3F01FFBFD705228777D1528A943B818A
SHA1:	08C01CA99807B70C41AC9A288BDA6EA7445B6009
SHA-256:	5B90DC28DE13FDA5DA1534245BD6FF18004ABF1D7D8AF70B1233D528732508A2
SHA-512:	8081252DDF0F94DC12F06FF05EB57EF019E092D189651B7EECEB8050159D460CEE7B4392BC859DCF523AE388D04B6A04B797BEB0E1E41732F922089C1148430
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":1.6567181986874e+12,"network":1.6566858e+12,"ticks":195698446.0,"uncertainty":3745423.0},"os_crypt":{"encrypted_key":"RFBbUEkBAAAA0lyd3wEV0RGMEgDAT8KX6wEAAABL95WKt94zTZq03WydzHLCAAAAAIAAAAAABBmAAAAAQAAIAAABAL2tyan+IsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAA6AAAAAAGAAIAAAABDv4gJLq1dOS7IkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAB045Od5v4BxiFP4bdRYjJdXn4W2fxYqQj2xfYeAnS1vCL4JXAsdflljw4oXIE4R7I0AAAABlT36FqChftM9b7EtaPw98XRXY944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDgb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639357535"},"plugins":{"metadata":{"adobe-flash-player":{"display

C:\Users\user\AppData\Local\Google\Chrome\User Data\e8b91c13-687e-4a5b-90e8-7c0373992032.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):	205766
Entropy (8bit):	6.042879056931
Encrypted:	false
SSDEEP:	6144:xogQRUdqIM7dKoOO2Z9gK1YcUaqfIUoOsiuRL:xNDdqe70oOI9gKVzo8
MD5:	15F7ECE6CA0CC5DF351D63FB869D886
SHA1:	8A72536B3792187C9564B03A10E60E6390A56880
SHA-256:	D949D4D7CD3AD9F929A5498E05151E5AE3EB41FCFE4FC6B239CEBEDBC4AC80DB
SHA-512:	088239D0A774A22E6F938FB531272D9F830B9A836972426D2C195882274BD08524378597F8E55FB0F740EA44D7862EE02A400CBD14C2E275A25CD651E90A2884
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":1.6567181986874e+12,"network":1.6566858e+12,"ticks":195698446.0,"uncertainty":3745423.0},"os_crypt":{"encrypted_key":"RFBbUEkBAAAA0lyd3wEV0RGMEgDAT8KX6wEAAABL95WKt94zTZq03WydzHLCAAAAAIAAAAAABBmAAAAAQAAIAAABAL2tyan+IsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAA6AAAAAAGAAIAAAABDv4gJLq1dOS7IkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAB045Od5v4BxiFP4bdRYjJdXn4W2fxYqQj2xfYeAnS1vCL4JXAsdflljw4oXIE4R7I0AAAABlT36FqChftM9b7EtaPw98XRXY944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDgb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13291230639357535"},"plugins":{"metadata":{"adobe-flash-player":{"display

C:\Users\user\AppData\Local\Google\Chrome\User Data\ec3a40c3-1400-4f01-815d-b48d30faaa73.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):	214206
Entropy (8bit):	6.07079771071813
Encrypted:	false
SSDEEP:	6144:GQogQRUdqIM7dKoOO2Z9gK1YcNaqfIUOoSiurL:GQNDdqe70oOI9gKVuo8
MD5:	DBC2001EFF8231AEC5FB53BEAB02A779
SHA1:	3CE65CD86017A3377A77B3D7BD81B19A1223BBE5
SHA-256:	9CECF660C23285CDB9862E8280198BD78733A98806B7529E667C586098F701BB
SHA-512:	474AB58E05FD68E8831579FC9F3DEACC042B34A277AB322EBAD561436A6F3FFCC8BF421D678A2D9E61A59C2B35EA10A900231F9BADA7030B309558E1FE28C6C4
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":"1.6567181986874e+12","network":"1.6566858e+12","ticks":195698446.0,"uncertainty":3745423.0},"os_crypt":{"encrypted_key":"RFBbUEkBAaaa0lyd3wEv0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAIAAAAAABBmAAAAQAIAAABAL2tyan+IsWtxhoUVdUYrYiwg8iJkppNr2ZbFie9UAAAAA6AAAAAaAIAAAABDv4gJLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXASdfjiw4oXIE4R7I0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGwCOPFyXOajfBL3GXBUhMXghJbDGB5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"display
----------	---

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\231C2286-1237-4321-A2E6-258BBA83D8CD	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	149155
Entropy (8bit):	5.356510256155895
Encrypted:	false
SSDEEP:	1536:9cQW/gxgB5BQguw5/Q9DQC+zQWk4F77nXmvid3Xx5ETLKz6e:sJQ9DQC+zPXwl
MD5:	BD30738058D1BB89A9729682E2BC0925
SHA1:	02B8BD201128A288DAF606A2E772685EA2A3388B
SHA-256:	2F749FD024D6222D14096E5E079FD1A34B3431573A2C9E2AC7797D7F44E2F3BB
SHA-512:	7BA656472EDD5AE092781D47DE985BCEA4C98EB7B3494ADE9FA18B2D4BFD6B48D1D69DC90BB91F9D39146F0217023AC2985ED0803E8D904FEE7BD8CA3371000
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">..<o:services o:GenerationTime="2022-07-01T14:28:43">..Build: 16.0.15427.30526-->..<o:default>..<o:ticket o:headerName="Authorization" o:headerValue="{}" />..</o:default>..<o:service o:name="Research">..<o:url>https://rr.office.microsoft.com/research/query.aspx</o:url>..</o:service>..<o:service o:name="ORedir">..<o:url>https://o15.officeredir.microsoft.com/r</o:url>..</o:service>..<o:service o:name="ORedirSSL">..<o:url>https://o15.officeredir.microsoft.com/r</o:url>..</o:service>..<o:service o:name="CIViewClientHelpId">..<o:url>https://[MAX.BaseHost]/client/results</o:url>..</o:service>..<o:service o:name="CIViewClientHome">..<o:url>https://[MAX.BaseHost]/client/results</o:url>..</o:service>..<o:service o:name="CIViewClientTemplate">..<o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>..</o:service>..<o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1A5C2F1B.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false
SSDEEP:	3:YmsaTILPtiN81HRQjIORGt7RQ//W1XR9//3R9//:r1912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB39E
Malicious:	false
Preview:	>.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FBE12F02.png 	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 1140 x 1281, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	912404
Entropy (8bit):	7.9907157898990695
Encrypted:	true
SSDEEP:	24576:lrQU57GpJk69mCNDPCBPY+bikHII5Bqn13dhWy:ay7jCIPsDJ55B67Wy
MD5:	8A82D12ADAF2E28F54C0C378CF009DA6
SHA1:	874AECC19A5756B367590CF31DD0B67D75F3AB21
SHA-256:	C626C48A60730CD0AEA01A1EBA366C8F6AA169E201A284244E18508D05BB4CEB
SHA-512:	97246B35130A6CC5E7A58E3A403B5FE162369FFF50E5F8B488F893B5D20BE27A941C679305EC7BD9AF4A63F06158C0A4F32377F835F44B2762366D51C4E8CAF1
Malicious:	false

SHA-256:	5424C7B084EC4C8BA0A9C69683E5EE88C325BA28564112CC941CD22E392D8433
SHA-512:	59DF2D5F2684FACC80C72F9C4B7E280F705776076C9D843534F772D5A3D578BEE04289AEE81320F23FB4D743F3969EDF5BA53FEBBAC8A4D27F3BC53BCF271CE
Malicious:	false
Preview:	{. "COMMENT": ["This file serves as a template for the resource info description used by ", . "the NaCl Chrome plugin. It is kept in the NaCl repository to prevent ", . "hard-coding of NaCl-specific information inside the Chrome repository.".], . "abi-version": 1, . "pnacl-arch": "x86-64", . "pnacl-ld-name": "ld.nexe", . "pnacl-llc-name": "pnacl-llc.nexe", . "pnacl-sz-name": "pnacl-sz.nexe", . "pnacl-version": "5dfe030a71ca66e72c5719ef5034c2ed24706c43".}

C:\Users\user\AppData\Local\Temp\1828_1378596767_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2712
Entropy (8bit):	3.4025803725190906
Encrypted:	false
SSDEEP:	48:b/5D5V5PK82aTS6aTTw0Do1DttoyDNsEA:b/hbVic1ZtLDNsE
MD5:	604FF8F351A88E7A1DBD7C836378AE86
SHA1:	9D8D89AE9F13D6306E619A4EAAD51EDE91A5F9F3
SHA-256:	947E64BE43E821562CE894F1AFCC3D09CD7FF614C107FC94250CD3EA5C943302
SHA-512:	85B1EDA4C473E00034EE627B7ABB894A77E521BC6A91A91A4A3744CA7511CB0AF10B9723D9ECC2CE3378DD70B659DF842D8C11875958CB77070CF01EC0A15840
Malicious:	false
Preview:	.ELF.....>.....@.....@.....PH.....,\$J! =...J.\$<A[. @.A...M..A..fffff.....PH.....,\$J! =...J.\$<A[.D..A...M..A..fffff.....PH..1...,\$J! =...J.\$<A[.....A...M..A..fffff.....PH..SP..h.....fff.....h.....fff.....J.\$<[.,\$J! =...J.\$<.....f.....NaCl....x86-64.....zR..x.....@.....C....C.....8.....@.....C....C.....T.....@.....C....Cp.....`....C....C..B.....<.....@.....X.....t.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl- clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pna

C:\Users\user\AppData\Local\Temp\1828_1378596767_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2776
Entropy (8bit):	3.5335802354066246
Encrypted:	false
SSDEEP:	48:b/5D5V5ej5ej5PjDdaTS6aTTw6DV1DtFouoyDOsTy:b/hbEEVJB1ZFhLDOsT
MD5:	88C08CD63DE9EA244F70BFC53BBCADF6
SHA1:	8F38A113A66B18BA02E2C995099CF1145A29DAA
SHA-256:	127F903CC986466AA5A13C17DFDD37AC99762F81A794180339069F48986BC7A3
SHA-512:	78D2500493A65A23D101EC2420DC5F0CE8C75EFAC425C28547121643E4FB568E9D827EF2C0F7068159E043C86B986F29BF92C6BADC675F160B63C7B3512EB95
Malicious:	false
Preview:	.ELF.....>.....X.....@.....@.....PH.....,\$J! =...J.\$<A[. @.A...M..A..fffff.....PH.....,\$J! =...J.\$<A[.D..A...M..A..fffff.....PH..1...,\$J! =...J.\$<A[.....A...M..A..fffff.....PH...,\$J! =...J.\$<A[f.....A...M..A..fffff.....PH...,\$J! =...J.\$<A[f.....A...M..A..fffff.....PH..SP..h.....fff.....J.\$<[.,\$J! =...J.\$<.....f.K.....P.....Z.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com /a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c9 4a3a7da70f0081724448f).....zR..x.....@.....C....C.....8.....@.....C....C.....T.....@.....C....C.....p.....@.....C....C.....@.....C....C.....@.....@...

C:\Users\user\AppData\Local\Temp\1828_1378596767_platform_specific\x86_64\pnacl_public_x86_64_crtend_o	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	1520
Entropy (8bit):	2.799960074375893
Encrypted:	false
SSDEEP:	12:Bvx/ekjIlM/NQqMTr9yp9396QqMTfR9C6wRqD8MTDDw7IEOkSbfuEAXwX6BX2U8b:bDjO/NbmT3296bmT3Twk8qDwh7b7CD8
MD5:	75E79F5DB777862140B04CC6861C84A7
SHA1:	4DB7BDC80206765461AC68CEC03CE28689BBEE0C
SHA-256:	74E8885B87ED185E6811C23942FD9BD1FBAC9115768849AF95A9DECFC6644B2EA
SHA-512:	FE3F86E926759E71494F2060C4ED3C883EBCAF20CB129A5AD7F142766C33FAB10B5FABC3C7C938E0E895E27EA0AC03CBFE8D0EEABF5300A4AD07F67FD96CC253
Malicious:	false

```
Preview: .ELF.....>.....@.....@.....NaCl.....x86-64.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git
ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7d70f0081724448f
)...text.comment.bss.group.note.GNU-stack.eh.frame.shstrtab.strtab.symtab.data.note.NaCl.ABI.x86-64.....!.....
...../././pnacl/support/crtend.c._EH_FRAME_END_.....
.....@.....H.....P.....H.....
```

[illegible]

C:\Users\user\AppData\Local\Temp\1828_1378596767_platform_specific\x86_64\pnacL_public_x86_64_libcrt_platform_a	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current archive
Category:	dropped
Size (bytes):	40552
Entropy (8bit):	4.127255967843258
Encrypted:	false
SSDEEP:	768:xlP+1fzyUNVU5LmKxeOnjpD5eA/eUnUUxvT:xlP+1ryMTekpD5eAWjuvT
MD5:	0CE951B216FCF76F754C9A845700F042
SHA1:	6F99A259C0C8DAD5AD29EE983D35B6A0835D8555
SHA-256:	7A1852EA4BB14A2A623521FA53F41F02F8BA3052046CF1AA0903CFAD0D1E1A7B
SHA-512:	7C2F9BF09EB1F43C17B4E14A077759FA9DC62A7239890975B2D6FD543B31289DC3B49AE456CA73B98DE9AC372034F340C708D23D9D3AAB05CCBDABDC56A634E
Malicious:	false
Preview:	!<arch>/ 0 0 0 0 624 `.....8...Z(..e..e...t..t..y'.y'.y'.y'.y'.y'.y'.y'.y'.y'.y'.y'.y'.y'.....fmod.fmodf.memcmp. memcpy.memmove.memset.__nacl_read_tp.__pnacL_init_irr.longjmp.setjmp.__Sz_fptosi_f32_i64.__Sz_fptosi_f64_i64.__Sz_fptoui_f32_i32.__Sz_fptoui_f32_i64.. __Sz_fptoui_f64_i32.__Sz_fptoui_f64_i64.__Sz_sitofp_i64_f32.__Sz_sitofp_i64_f64.__Sz_uiofp_i32_f32.__Sz_uiofp_i32_f64.__Sz_uiofp_i64_f32.__Sz_uiofp_i64_f64.n acl_tp_tdb_offset.nacl_tp_tls_offset.__Sz_bitcast_16xi1_i16.__Sz_bitcast_8xi1_i8.__Sz_bitcast_i16_16xi1.__Sz_bitcast_i8_8xi1.__Sz_fptoui_4xi32_f32.__Sz_uiofp_4 xi32_4xf32.e_fmod.o/ 0 0 0 644 2792 `.ELF.....>.....@.....@.....PH.AVAUATSfl~.M..I..E....@. A.....D..D1.....8fl~.M.....I.. E..A.....D..D..t.D....D..f....D.=...r..Y...^[AA]A^..@...\$.I =...J.\$<A[A...M..

C:\Users\user\AppData\Local\Temp\1828_1378596767_platform_specific\x86_64\pnacL_public_x86_64_libgcc_a	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	132784
Entropy (8bit):	3.6998481247844937
Encrypted:	false
SSDEEP:	384:Hf0mOXymeKzQUldedRFvT5p1Ee2HyAIL3O4:Hf7OXdmWRJT5p1R2HyAhO4
MD5:	C37CA2EB468E6F05A4E37DF6E6020D0F
SHA1:	EA787E5EADFB488632EC60D8B80B555796FA9FE9
SHA-256:	C1483ED423FEE15D86E8B5D698B2CDAB89186CE7FF9C4E3D5F3F961FD80D7C6E
SHA-512:	01281DE92B281FB29E1ACA96AA64B740B65CC3A9097307827F0D8DB9E1C164C56AFCDFA0BF138EA670A596D55CE2C8D722760744E9FC9343BB6514417BF33E8A
Malicious:	false

Preview:	!<arch>./ 0 0 0 0 942 `.....4..x.#...-4l.E..M...U...].n...u...-X...4.....L.....t...p.....`.....".....*...1.....D...K...T...l...d...r...].j0.....x.....L.....\..8.....clzti2.__compilerrt_fmax.__compilerrt_fmaxf.__compilerrt_logb.__compilerrt_logbf.__ctzti2.__divdc3.__divdi3.__divmoddi4.__divmodsi4.__divsc3.__divsi3.__divti3.__fixdfdi.__fixdfsi.__fixdfti.__fixsfdi.__fixsfsi.__fixsfti.__fixunsdfdi.__fixunsdfsi.__fixunsdfti.__fixunssfdi.__fixunssfsi.__fixunssfti.__floatdidf.__floatdisf.__floatsidf.__floatsisf.__floattidf.__floattisf.__floatundidf.__floatundisf.__floatunsidf.__floatunsisf.__floatuntidf.__floatuntisf.compilerrt__abort_impl.__moddi3.__modsi3.__modti3.__muldc3.__muloti4.__mulsc3.__multi3.__popcountdi2.__popcountsi2.__popcountti2.__powidf2.__powisf2.__udivdi3.__udivmoddi4.__udivmodsi4.__udivmodti4.__udivsi3.__udivti3.__umoddi3.__umodsi3.
----------	--

C:\Users\user\AppData\Local\Temp\1828_1378596767\platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	13514
Entropy (8bit):	3.8217211433441904
Encrypted:	false
SSDEEP:	192:uU9v4pXizdrEuxwk3vp20tprpdSGFwDqO:P9v4palvvc0tpFdSGFwmO
MD5:	4E8BEDA73EB7BD99528BF62B7835A3FA
SHA1:	DC0F263A7B2A649D11FF7B56FE9CFAC44F946036
SHA-256:	6B835FD48DF505EB336FF6518CE7B93BB0ED854DADAA5C1EEED48D420291F62C
SHA-512:	46116B8BABC719676D68FD40D2AC82F38A3D13D8A482ADFC6FC32A99170AC3420E52CC33242CCD0FA723ABF4FA5EDBB9CE16A09C729BF04AE4AFBB2F67A1F38B
Malicious:	false
Preview:	!<arch>./ 0 0 0 0 94 `....._pnacl_wrapper_start.__pnacl_real_irt_query_func.__pnacl_wrap_irt_query_func.shim_entry.o/ 0 0 0 644 7392 `..ELF.....>.....@.....@.....NaCl....x86-64.....A.L....A.L...D.....D....A.....t+.. u..t"...A.D.....A... ..A.D.....f..D.<.....Q.....V.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f)...!../ppapi/native_client/src/untrusted/pnacl_irt_shim/shim_entry.c/mnt/data/b/build/slave/sdk/build/src/out_pnacl/x64.NACL_STARTUP_FINI.NACL_STARTUP_ENVVC.NACL_STARTUP_ARGC.NACL_STARTUP_ARGV.NaClStartupInfoIndex.unsigned int.size_t.char.TYPE_na

C:\Users\user\AppData\Local\Temp\1828_1378596767\platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	2078
Entropy (8bit):	3.21751839673526
Encrypted:	false
SSDEEP:	24:MOcpdhWE5O/bZbmT3296bmT3TwQwDnvD/+R3:MHuECdaTS6ATTwXDvD/+I
MD5:	F950F89D06C45E63CE9862BE59E937C9
SHA1:	9CFAD34139CC428CE0C07A869C15B71A9632365D
SHA-256:	945B1C8A1666CBF05E8B8941B70D9D044BAAFB59B006F728F8995072DE7C4C40
SHA-512:	F9AFBB800A875EDCC63DEA4986179E73632B3182951A99C8B3D37DB454EFD7CC7192ECA5AC87514918A858BAD6DAEAB59548CA2E90EADA9900EF5B9F08E62CFC
Malicious:	false
Preview:	!<arch>./ 0 0 0 0 30 `....._pnacl_wrapper_start.// 20 `..dummy_shim_entry.o/.0 0 0 644 1840 `..ELF.....>.....@.....@.....PH.....\$J.I=....J.\$<.....f..D.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).....zR..x.....C....C.....rela.text..comment..bss..group..note.GNU-stack..rela.eh_frame..shstrtab..strtab..symtab..data..note.NaClABI.x86-64.....

C:\Users\user\AppData\Local\Temp\1828_1378596767\platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe 	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=309d6d3d463e6b1b0690f39eb226b1e4c469b2ce, stripped
Category:	dropped
Size (bytes):	14091416
Entropy (8bit):	5.928868737447095
Encrypted:	false
SSDEEP:	196608:tKVqXp3Qev4dg6iIfHM8KLM2J3jqjnkZ:uqufB
MD5:	9B159191C29E766EBBF799FA951C581B
SHA1:	D1D4BBC63AB5FC1E4A54EB7B82095A6F2CE535EE
SHA-256:	2FA4A3A0730142C5EE4FA2C05D27A5DEFC18886A382D45F5DB254B61B28ED642B
SHA-512:	0B4FF60B5428F81B8B1BCF3328CF80CBD88D8CE5E8BDBC236B06D5A54E7CF26168A3ABB348D87423DA613AB3F0B4D9B37CB5180804839F1CA158EC2B315DD00
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\1828_1378596767_platform_specific\x86_64\pnacL_public_x86_64_pnacL_sz_nexe	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=4b15de4ab227d5e46213978b8518d53c53ce1db9, stripped
Category:	dropped
Size (bytes):	1901720
Entropy (8bit):	5.955741933854651
Encrypted:	false
SSDEEP:	12288:gXqUSPbjwQO2o8k+7zjdg4euCAauOILfvCpGy4Wh3BTFmHppq82K2/KsvPyla9d:gafZwcOdNe2auOepCBTfMjq3Kf8ksr
MD5:	9DC3172630E525854B232FF71499D77C
SHA1:	0082C58EDCE3769E90DB48E7C26090CE706AD434
SHA-256:	6AA1DA6C264E0AF4E32A004F4076C7557C6AC6D9C38B0C5DE97302D83FA248C3
SHA-512:	9E9584241A39EED1463D7D4C1B26AE570B839AA315778FF3400C61341EBA43B630307DE9F1532A265CA82EA69BDEA03EC9D963E59A18569C02DA8285449870F1
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	.ELF.....>.....@.....@.8...@.....0....0.....Y.....@.....@.....P.td....t^.....t^.....W.....W.....Q.td.....NaCl...x86-64.....GNU.K..J..'..b.....<S...`'...'..@.. @.....@.....Y@.....p.....@.....?.....?.....A.....5...?5.5...?5...?.....P9.....PC.....?.....0@.....aCoc?...?(..? .y.P.D.?<s.O.u.....\$@.....@.....@.....@.....@.....@.....@.....@.....Z...[...[...e..... ..@... ..@.. `.....0...0..2.`4.. 6...7...9...~...~...z...{...{..

C:\Users\user\AppData\Local\Temp\1828_1378596767\manifest.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	573
Entropy (8bit):	4.859567579783832
Encrypted:	false
SSDEEP:	12:BLqG6yDJmL4mLDIG9hQ181G46XzrXc+EFFnQpaiOc+T5NqXIOclNqXL:BkylmL4mLDIJ18116XsRNqtZeNqXIZIE
MD5:	1863B86D0863199AFDA179482032945F
SHA1:	36F56692E12F2A1EFCA7736C236A8D776B627A86
SHA-256:	F14E451CE2314D29087B8AD0309A1C8B8E81D847175EF46271E0EB49B4F84DC5
SHA-512:	836556F3D978A89D3FC1F07FCED2732A17E314ED6A021737F087E32A69BFA46FD706EBBDFD3607FF42EDCB75DC463C29B9D9D2F122504F567BB95844F579831
Malicious:	false
Preview:	{."update_url": "https://clients2.google.com/service/update2/crx"... "description": "Portable Native Client Translator Multi-CRX",. "name": "PNaCl Translator Multi-CRX",. "manifest_version": 2,. "minimum_chrome_version": "30.0.0.0",. "version": "0.57.44.2492",. "platforms": [{. "nacl_arch": "x86-32",. "sub_package_path": "_platform_specific/x86_32",. }, {. "nacl_arch": "x86-64",. "sub_package_path": "_platform_specific/x86_64",. }, {. "nacl_arch": "arm",. "sub_package_path": "_platform_specific/arm",. }]}.

Process:	C:\Program Files\Google\Chrome\Application\chrome.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:	EA1C1FFD3EA54D1FB117BFDDB3569C60
SHA1:	10958B0F690AE8F5240E1528B1CCFFFF28A33272
SHA-256:	7C3A6A7D16AC44C3200F572A764BCE7D8FA84B9572DD028B15C59BDCCBC0A77D
SHA-512:	6C30728CAC9EAC53F0B27B7DBE2222DA83225C3B63617D6B271A6CFEDF18E8F0A8DFFA1053E1CBC4C5E16625F4BBC0D03AA306A946C9D72FAA4CEB779F8F8CAF
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 lp..>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.lSa...)....H.&92..?l..~..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.@ ^.l.<A..J..j.'.G.`.\$q.N..Tdq]2jp.OF.#.#.....'.....8.3.....0..0...*H.....0.....O..(.....'19..O/>.....=...m.n.l.z.q.....JW..F.....+H.Z+KGQ.9.....8.....U...&y.....\$...?Eo.....\f/Z..+M8...B.3'.Y.f..X.AS?~..k.k.n.....Z...&G....."n.....l.Ov.x#<...Lx..-w..-..d.....J.pT..('e~*{qkQ.Q.....rl.....Z...v.N.....J.d.....rX.....w@..b.[c..lV'.c..l..~.k..}z...U.S..nC.....@.....Y...#D.z.....5&1O...X=p..2.F..P.6yP..>{.....HBX.*E5...y..

C:\Users\user\AppData\Local\Temp\1828_877695470_metadata\verified_contents.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):	1765
Entropy (8bit):	6.027545161275716
Encrypted:	false
SSDEEP:	48:p/hii6zkv/Vl1Jip2qRNVhakuQkCNFxdSgwmBKkgum91:Rz0kv6cNvaYNFWSEhug
MD5:	45821E6EB1AEC30435949B553DB67807
SHA1:	B3CADEB17FE5B76B5DBB428B8D3A07B341F8B1BC
SHA-256:	E5FAE91295BECF7F66BFA4BE1061CA5537ED763EB5D01485F23ECFB583304FEE
SHA-512:	BCBE40CAFAAA4B14566D91E361D8FB7F0288D5C459FA478AA4C575444DA4D406E1076FC0B3A31D4A9E5EE034F0FE15A0EFE8A8A52B838DE94B96D3E488D28FCE
Malicious:	false
Preview:	[{"description": "treehash per file", "signed_content": {"payload": "eyJjb250ZW50X2hhc2hlcy6W3siYmxvY2tfc2I6ZSI6NDANiwiZGlnZXN0Ijoic2hhMjU2IiwizmlsZXMiOlt7InBhdGciOiJSZWVndmVyeS5jcngzliwicm9vdF9oYXNoljoiaGdCR051SzhNR2NKaDIlfNmZQAfdEWmpVYUfKeklzleDJJS21DUEZvb0dfUSJ9LHsicGF0aCI6Im1hbmdlZXN0Lmpzbn24ilClJyb290X2hhc2giOiIwYXduVFBFQmdDRHkyV05hVvk3Um9mSWN3c3ZwNHFRnUXzVMxvXRiVXY0ln1dLCJmb3JtYXQiOiJ0cmVlaGFzaCIslmhhc2hfYmxvY2tfc2I6ZSI6NDASnn1dLCJpdGVtX2lkIjoiaWhubGNlbm9jZWhnZGFIZ2RtaGJpZGpobmhkyY2hmboiLjMuMzYuMTQxLiwiCHJvdG9jb2xfdmVyc2lvbi6MX0", "signatures": [{"header": {"kid": "publisher"}, "protected": "eyJhbGciOiJSuz1NiJ9", "signature": "iFuMX_koz-zJ7KVu6Lxb3rHWZgQvk2hv25x_SGBiDV_okALrGbj6rUOWyNNNsHXMNt118XZmA696XR8qkr4dwT5Gvez-9gi-WYBY7XBkgo7v6NspGgJF89BNCel-P9k-zBHOGrf-fCEiAcoM7xCx9_f8qlRy7nhQPjyOIhn5eJEir0uSu6gdqR9afnYZ3Uor-VOLDObt7fA4ee38MP2ut5qWU50F5dvlezfKktVDMHwztvcLYc6R9SVkdSYv6jvwWGccYRI-aclvkkHu6SnbZGI7fmDZdkcBAxBHYEZZMMmvb76ro4SO15GDyEVAo_Q4f4trdr_Y_GyN_Bm73imCTjgtoGc"}]}

C:\Users\user\AppData\Local\Temp\1828_877695470\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.7900469623255675
Encrypted:	false
SSDEEP:	3:SpOXzxIQ4BdPWfDL9c:SpOjDQFVc
MD5:	2AE14F91312C4E8034366B09D49D5B18
SHA1:	AD4933A5D838D0FA0B960C327A5039A9E8249642
SHA-256:	4F122332EF0F2BB490EF59619D3602C1A7277C0A7A19C132202DB4803A09BFA2
SHA-512:	FB0CC467A4B8463F6A3BF42CDC11C23B34EB94A9397644B68714DCB819EE326BAE05022D59D23DC9907DF1E6928064D853FD0900BB6083417892D4D5A9BA771
Malicious:	false
Preview:	1.aeedb246d19256a956fedaa89fb62423ae5bd8855a2a1f3189161cf045645a19

C:\Users\user\AppData\Local\Temp\1828_877695470\manifest.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	195
Entropy (8bit):	4.682333395896383

Encrypted:	false
SSDEEP:	3:rR6TAulhFphifJ9LAG9Xg0XTFHqS1wP/pEeSWU4pv/8F/FxLj2RF2fcTZTotL:F6VIM90ggiTgS1wnuWfB0NpK4aotL
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\Local\Temp\3a6ddb19-0e1b-45fc-b970-e7ff4e6406ca.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCDB92598A0F13D313CC9EBC2A07E61F007BAF58FBFB94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Temp\cfba26a0-2d5f-46ad-b890-a1b6725a941d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCIuXZSk+QSVh85PxEalRVHmclD9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99FId9RBQYBVcaxInfl
MD5:	541F52E24FE1EF9F8E12377A6CCAEOC0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCFA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Preview:	Cr24.....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.....\..Fl...b...l5....zJ.q.....L]....w[T0.6...E.....r.%Z.vFm.9..5!,-g5...;t...']...+A.....u..k..e..&.l.6r[yU...%.f.....N..V.....<+.....l.},{...z...)y.n..').....,b...5.08K%.O.g..D.S.F5o..<(....>...f.X..l..2."l..w...7f ~.c.4.E.....0.0...*H.....0.....)'..b.*\$w\$.q&.]zF_2...;...?U,...W..L1.2...R..#...W....c1k.\$W..\$.J....+M!.Hz.n'U.I)N. b.l.....{K@[6.LIP/....](A.....0.....l....)H....IQ.y.;MG.d..ix.#f.Z\$[.].?...0K...t'i..s...Y..%.Ky....0...{!+.-v.;....J....Z....)(6..@?v;.-.2..c....[0Y0*..H.=...*.H.=...B.....r...2..+Y.l...k..bR.j5Sl..8.....H'i..l..`Q{...F0D..0...}!.A..L.+.=...kP.!1..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOIf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F7700C
Malicious:	false

Preview:	{.. "app_description": {.. "message": "..... .. Chrome".. },.. "app_name": {.. "message": "..... .. Chrome".. },.. "crawl_app_unavailable": {.. "message": "..... .. Chrome".. },.. "crawl_connect_to_network": {.. "message": "..... .. Chrome".. },.. "iap_unavailable": {.. "message": "..... .. Chrome".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... .. Chrome".. },..}
----------	---

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CB4
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "crawl_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "crawl_connect_to_network": {.. "message": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. },..}

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEI4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488CB
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "crawl_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn.".. },.. "crawl_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. },..}

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJMKKFZGGJMKKFZ+WYpU34OHu+dgxICZ08ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5E0A
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Betaling i Chrome Webshop".. },.. "app_name": {.. "message": "Betaling i Chrome Webshop".. },.. "crawl_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i jeblikket.".. },.. "crawl_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betal i appen er ikke tilg.ngelig i jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. },..}

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\de\messages.json	
---	--

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMICTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Beww8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80552
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. }... "app_name": {.. "message": "Chrome Web Store-Zahlungen".. }... "crawl_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. }... "crawl_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. }... "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. }... "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWIOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD994983BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B40
Malicious:	false
Preview:	{.. "app_description": {.. "message": "..... Chrome Web Store".. }... "app_name": {.. "message": "..... Chrome Web Store".. }... "crawl_app_unavailable": {.. "message": "..... Chrome Web Store".. }... "crawl_connect_to_network": {.. "message": "..... Chrome Web Store".. }... "iap_unavailable": {.. "message": "..... Chrome Web Store".. }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. }... "please_sign_in": {.. "message": "..... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. }... "app_name": {.. "message": "Chrome Web Store Payments".. }... "crawl_app_unavailable": {.. "message": "App currently unavailable.".. }... "crawl_connect_to_network": {.. "message": "Please connect to a network.".. }... "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. }... "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526

Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A976D929FEFEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "crawl_app_unavailable": {.. "message": "App currently unavailable".. },.. "crawl_connect_to_network": {.. "message": "Please connect to a network".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. },.. "please_sign_in": {.. "message": "Please sign into Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbgGHIb+WYpU34ubdDH+dgxbFxTO8ZpU34IPbdIVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNI5OGAOfFD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1AC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE0128
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "crawl_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento".. },.. "crawl_connect_to_network": {.. "message": "Con.ctate a una red".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\es_419\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbgGHIb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LIOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEB7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA53
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "crawl_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento".. },.. "crawl_connect_to_network": {.. "message": "Con.ctate a una red".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. },.. "please_sign_in": {.. "message": "Accede a Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgRW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqIWYpTeObk8ZpT/OGAOfuLIR
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD

SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. }... "app_name": {.. "message": "Chrome'i veebipoe maksed".. }... "crawl_app_unavailable": {.. "message": "Rakendus pole praegu saadaval".. }... "crawl_connect_to_network": {.. "message": "Looge .hendus v.ruga".. }... "iap_unavailable": {.. "message": "Rakendusesised maksed ei ole praegu saadaval".. }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. }... "please_sign_in": {.. "message": "Logige Chrome'i sisse".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\fi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BED8
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. }... "app_name": {.. "message": "Chrome Web Storen maksut".. }... "crawl_app_unavailable": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. }... "crawl_connect_to_network": {.. "message": "Muodosta verkkoyhteys".. }... "iap_unavailable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. }... "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\fil\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	12:1HEJADlbgGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfV:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF52
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. }... "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. }... "crawl_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app..".. }... "crawl_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network..".. }... "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App..".. }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. }... "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\fr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	677
Entropy (8bit):	4.552569602149629
Encrypted:	false
SSDEEP:	12:1HEJAlf/nbGGAlf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03OyZnLAO8:1HE4Hna1Hn6WYpNdgpy8ZpSTQwnBOGAh
MD5:	8D11C90F44A6585B57B933AB38D1FFF8
SHA1:	3F9D44EA8807069A32AACA2AAAD02FD892E6CC90
SHA-256:	599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5
SHA-512:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F7
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. }... "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. }... "crawl_app_unavailable": {.. "message": "Application indisponible pour le moment..".. }... "crawl_connect_to_network": {.. "message": "Veuillez vous connecter . un r.seau..".. }... "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment..".. }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed..".. }... "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\hi\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.791154467711985
Encrypted:	false
SSDEEP:	24:1HEs07J0JWYp9vnCSVLP8Zp6CsOGAOf8SLm:Wh7qgYp1CMLUph1GiSLm
MD5:	E376D757C8FD66AC70A7D2D49760B94E
SHA1:	1525C5B1312D409604F097768503298EC440CC4D
SHA-256:	8106D98C4F8DA16DB698444409558E29CC96735E188BFA303C333A5D99231C1D
SHA-512:	673F3F259AF2946E4F49BBED14A2A70D44BF9FDA9D7A71DC9172BA9B7B3C7F7062B16D29682B638D485B0520ED6F99E7A735F28C7C719B539559005B69FA755F
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome" .. }.. "app_name": {.. "message": "Chrome" .. }.. "crawl_app_unavailable": {.. "message": "..... .." .. }.. "crawl_connect_to_network": {.. "message": "..... .." .. }.. "iap_unavailable": {.. "message": "..... .." .. }.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed." .. }.. "please_sign_in": {.. "message": "..... Chrome" .. }..}

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\hr\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	618
Entropy (8bit):	4.56999230891419
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphK:1HE4H4TH8WYpNjTta28ZpQVLP0SOGAOK
MD5:	8185D0490C86363602A137F9A261CC50
SHA1:	5BD933B874441CEACB9201CCC941FF67BAED6DC0
SHA-256:	A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15
SHA-512:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D096E
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. }.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. }.. "crawl_app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna." .. }.. "crawl_connect_to_network": {.. "message": "Pove.ite se s mre.om." .. }.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno." .. }.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed." .. }.. "please_sign_in": {.. "message": "Prijavite se na Chrome." .. }..}

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\hu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	683
Entropy (8bit):	4.675370843321512
Encrypted:	false
SSDEEP:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfGijO8ZpU34Huo9O03OyZnLAOfTYBIAym:1HEVrk5WYpQzTUg/8ZpwoXOGAOfYIAd
MD5:	85609CF8623582A8376C206556ED2131
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. }.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. }.. "crawl_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el." .. }.. "crawl_connect_to_network": {.. "message": "K.rj.k, csatlakozzon egy h.i.zathoz." .. }.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el." .. }.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed." .. }.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba." .. }..}

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	4.465685261172395

Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyZnLAOfTYR:1HEBaA6WYpaHFH8ZptOYOGAOf2D
MD5:	EAB2B946D1232AB98137E760954003AA
SHA1:	60BDC2937905B311D2C9844DF2D639D7AC9F7F67
SHA-256:	C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3
SHA-512:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA12
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "crawl_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini".. },.. "crawl_connect_to_network": {.. "message": "Sambungkan ke jaringan".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.479418964635223
Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OyZnLAOfTYsD:1HEXd/aKd/6WYpZrv58ZpskOGAOfzD
MD5:	A328EEF5E841E0C72D3CD7366899C5C8
SHA1:	2851ED658385804E87911643F5A4200B1FB26E13
SHA-256:	CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D
SHA-512:	E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "crawl_app_unavailable": {.. "message": "App al momento non disponibile".. },.. "crawl_connect_to_network": {.. "message": "Collegati a una rete".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non al momento disponibile".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. },.. "please_sign_in": {.. "message": "Accedi a Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.20469020877498
Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4C6
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome". },.. "app_name": {.. "message": "Chrome". },.. "crawl_app_unavailable": {.. "message": ".....". },.. "crawl_connect_to_network": {.. "message": ".....". },.. "iap_unavailable": {.. "message": ".....". },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. },.. "please_sign_in": {.. "message": "Chrome". }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\ko\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	631
Entropy (8bit):	5.160315577642469
Encrypted:	false
SSDEEP:	12:1HEJ1GG1+WYpU34K3aT+dgh8d0HTO8ZpU34KaNkaT03OyZnLAOfTY/YeHx:1HEajWYpc3aSl0Hq8Zpc6kasOGAOfyYA
MD5:	9F6B4D82A70C74CA751E2EAE70FAB5CF
SHA1:	0534F125FFCE8222277CF2BE3401C59DAF9217F8
SHA-256:	D1467B8D037114403E8F4EFC52E88C4A7FEB96126BE4CFF883FEFF1084EF7E68
SHA-512:	ED9319830314385D09C06F62EE34186E8CA576C857981205E4468A28B3ACD2AB03384E77B866032C324ABDD97A56EFD08E2D6E0C79D563578B3EC52517819BD
Malicious:	false

Preview:	{.. "app_description": {.. "message": "Chrome" }.. "app_name": {.. "message": "Chrome" }.. "crawl_app_unavailable": {.. "message": ". " }.. "crawl_connect_to_network": {.. "message": "..... .." }.. "iap_unavailable": {.. "message": ". " }.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. }.. "please_sign_in": {.. "message": "Chrome.".. }..}
----------	---

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\lt\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	4.66839186029557
Encrypted:	false
SSDEEP:	12:1HEJpqHnkGqHnk+WYpU346M+dgV6O8ZpU34WzSWz03OyZnLAOfTYx:1HELqHtkQHPWYpM3A8ZpwGzOGAOfg
MD5:	4CA644F875606986A9898D04BDAE3EA5
SHA1:	722A10569E93975129D67FBD875B537D9D622AD1
SHA-256:	7C311AB751D840D750C11553C083785813E079C1D464FE568A98C9E3EF3DB96C
SHA-512:	E575E3D0622F5BD4B6C0EE79128A1B1F1882195670139D1983F4377D847141B8FB8EBB8BCED82AF3A220ED07D3577AFBE085BADC0E9C7678292B80E3EC5D344
Malicious:	false
Preview:	{.. "app_description": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. }.. "app_name": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. }.. "crawl_app_unavailable": {.. "message": "Programa .iuo metu negalima.".. }.. "crawl_connect_to_network": {.. "message": "Prisijunkite prie tinklo.".. }.. "iap_unavailable": {.. "message": "Mok.jimai programoje .iuo metu negalimi.".. }.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. }.. "please_sign_in": {.. "message": "Prisijunkite prie .Chrome..".. }..}

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\lv\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	671
Entropy (8bit):	4.631774066483956
Encrypted:	false
SSDEEP:	12:1HEJFhVbGGFhVb+WYpU34wDoz+dgGedB08ZpU34wF03OyZnLAOfTYGYID:1HENQKkWYp2Doy/em8Zp2WOGAOfRYID
MD5:	C5CE2C51391EAFD3DA9E4C71549A3C28
SHA1:	1F67FF6EF6E90C0CE3AAF56ED543A3EFD381574D
SHA-256:	1FA1DF2CA8516DEF490FB8484E9AA498ACFF80EEF5C9258FFE42D3678E6C7DED
SHA-512:	C85F6281E682F52BC2147DEA7E2F3BB4DC48D98BADA8687B05C6C7271C78EA7F5431CD51671A4184C9AE004FC53C016E3C594697F483195CCBA08A93821EEF0
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. }.. "app_name": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. }.. "crawl_app_unavailable": {.. "message": "Lietotne pagaid.m nav pieejama.".. }.. "crawl_connect_to_network": {.. "message": "L.dzu, izveidojiet savienojumu ar t.klu.".. }.. "iap_unavailable": {.. "message": "Maks.jumi lietotn.s pa.laik nav pieejami.".. }.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. }.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome..".. }..}

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\nb\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.555032032637389
Encrypted:	false
SSDEEP:	12:1HEJhiOGGhiO+WYpU34OHSN+dgFjdGFZO8ZpU34JgdN03OyZnLAOfTYiD:1HEDiHliWYpCYJ8ZpD1OGAOfRD
MD5:	93C459A23BC6953FF744C35920CD2AF9
SHA1:	162F884972103A08ADB616A7EB3598431A2924C5
SHA-256:	2CD700AEB57D89C2E73333D0702556EE3FF3863516170F85669BC680FCBDC4E0
SHA-512:	F76E68D8499306883C3EC1E774F7E8BB6B601096DA5A14D17D3E7D5732829542041E42B7350466589291ADCC83FB065FD591B4E20CFCF8EDC586E128ECBFCF5
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Chrome Nettmarked-betalinger".. }.. "app_name": {.. "message": "Chrome Nettmarked-betalinger".. }.. "crawl_app_unavailable": {.. "message": "Appen er utilgjengelig for .yeblikket.".. }.. "crawl_connect_to_network": {.. "message": "Du m. koble til et nettverk.".. }.. "iap_unavailable": {.. "message": "Betalning i app er ikke tilgjengelig for .yeblikket.".. }.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. }.. "please_sign_in": {.. "message": "Du m. logge p. Chrome..".. }..}

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\nl\messages.json	
---	--

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	615
Entropy (8bit):	4.4715318546237315
Encrypted:	false
SSDEEP:	12:1HEJJQGkbGGJQGkb+WYpU34OQKJT+dgiXUmvFZO8ZpU34g7JT03OyZnLAOfTYMD:1HErxkaqxk6WYptndXI8ZpTOGAOfbD
MD5:	7A8F9D0249C680F64DEC7650A432BD57
SHA1:	53477198AEE389F6580921B4876719B400A23CA1
SHA-256:	92BE7C2DC9CFBE5A65E9CE6488D364C8D7EC19E7B67A31E4D43C1CB2B169671C
SHA-512:	969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8/A7
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Betalingen via Chrome Web Store".. },.. "app_name": {.. "message": "Betalingen via Chrome Web Store".. },.. "crawl_app_unavailable": {.. "message": "App momenteel niet beschikbaar.".. },.. "crawl_connect_to_network": {.. "message": "Maak verbinding met een netwerk.".. },.. "iap_unavailable": {.. "message": "In-app-betalingen is momenteel niet beschikbaar.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log in bij Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\pl\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.646901997539488
Encrypted:	false
SSDEEP:	12:1HEJbivbGGbivb+WYpU34OBHIBi9+dgQUg6O8ZpU34bdbfilu03OyZnLAOfTYR5k:1HE5iVauiv6WYpIAyR8ZpxFiaOGAOfiC
MD5:	0E6194126AFCCD1E3098D276A7400175
SHA1:	E8127B905A640B1C46362FA6E1127BE172F4A40F
SHA-256:	E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C17A3943A6373C2
SHA-512:	A71F7C7BFBBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADF81271E1775C9BA299F6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B777
Malicious:	false
Preview:	{.. "app_description": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "app_name": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "crawl_app_unavailable": {.. "message": "Aplikacja jest obecnie niedost.pna.".. },.. "crawl_connect_to_network": {.. "message": "Po..cz si. z sieci..".. },.. "iap_unavailable": {.. "message": "P.atno.ci w ramach aplikacji s. teraz niedost.pne.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\pt_BR\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	636
Entropy (8bit):	4.515158874306633
Encrypted:	false
SSDEEP:	12:1HEJsc/bGGsc/b+WYpU34OLw+dgn/KzO8ZpU34FjIBmWGRO03OyZnLAOfTYN+KcY:1HEb/a8/6WYp4mZ8Zp7cKIOGAOf2iD
MD5:	86A2B91FA18B867209024C522ED665D5
SHA1:	63DEC245637818C76655E01FCB6D59784BC7184E
SHA-256:	6374880FDD1F8AF1EE8AEA6A06B73BE0AB265AFCEB4FE6F08BDE3B3989264B21
SHA-512:	DA6DBDE5028756421C2904F605632EE98831A25A1247E6238A931629B94CE8A00FD76F4235F118D2167304BD60F2C06B2AD78E54FF6CE53F8C38DF8C7B5AFCE
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pagamentos da Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos da Chrome Web Store".. },.. "crawl_app_unavailable": {.. "message": "Aplicativo indispon.vel no momento.".. },.. "crawl_connect_to_network": {.. "message": "Conecte-se a uma rede.".. },.. "iap_unavailable": {.. "message": "No momento, os Pagamentos no aplicativo n.o est.o dispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Fa.a login no Google Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\pt_PT\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	622
Entropy (8bit):	4.526171498622949
Encrypted:	false

SSDEEP:	12:1HEJsZUkbGGsZUkb+WYpU34OAE+dgqxKzO8ZpU34rEpBfvPO03OyZnLAOfTYLD:1HEmUka5Uk6WYpFvdxZ8ZpStnPIOGAOS
MD5:	750A4800EDB93FBE56495963F9FB3B94
SHA1:	8BFB915488A4EB3CB33D68E2E59F1F8447DB7D61
SHA-256:	C1C94F65FABAF17DEF98A8587711A56D61B1E5607500E9B01F2824DB109F9E83
SHA-512:	2AEDEF5793406221BE76AF22031CE8C30AB5FAEAD09BB394C153E2EBE990C89C1A2A73B40D8A92842641AFCa8C77FFD808A2058602D3646FD8DAE2844406F24
Malicious:	false
Preview:	{.. "app_description": {.. "message": "Pagamentos via Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos via Chrome Web Store".. },.. "crawl_app_unavailable": {.. "message": "Aplica..o atualmente indispon.vel".. },.. "crawl_connect_to_network": {.. "message": "Ligue-se a uma rede".. },.. "iap_unavailable": {.. "message": "Os Pagamentos na app est.o atualmente indispon.veis".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. },.. "please_sign_in": {.. "message": "Inicie sess.o no Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\ro\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.61125938671415
Encrypted:	false
SSDEEP:	12:1HEJqJrJZGGqJrJZ+WYpU344Hlx2Z+dgvrPIZO8ZpU34qT7hl3O03OyZnLAOfTYU:1HEC4D8WYpKow8WV68ZpKhoOGAOfVGD
MD5:	98D43E4B1054A65DF3FA3CC40AB6FB6D
SHA1:	46E0A21C4DA2BB5D4D8F837AE211C1B6FA26E7E2
SHA-256:	113A13900CBA62FE8AED06751971C23A80A99B47F9BE219CF884D57DB19611D9
SHA-512:	A76DC53912A4F46714926B9EA2B22E909540E447F61F6DD72607AB7B3BB5D4A9B39E525B04C33AEC53BA813D14AC1FB5827275B2524E52B693E83171E1CD146F
Malicious:	false
Preview:	{.. "app_description": {.. "message": "PI..i prin Magazinul web Chrome".. },.. "app_name": {.. "message": "PI..i prin Magazinul web Chrome".. },.. "crawl_app_unavailable": {.. "message": ".n prezent, aplica.ia nu este disponibil".. },.. "crawl_connect_to_network": {.. "message": "Conectear.-te la o re.ea".. },.. "iap_unavailable": {.. "message": "PI..ile .n aplica.ie nu sunt disponibile momentan".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. },.. "please_sign_in": {.. "message": "Conectear.-te la Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\ru\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	744
Entropy (8bit):	4.918620852166656
Encrypted:	false
SSDEEP:	12:1HEJ7OJHZMSI3ZGG7OJHZMSI3Z+WYpU34zWJ2F+dgVtLSv/TO8ZpU347NWJT03On:1HEIOJHZMq4uOJHZMq8WYpdWJ/YGHq8m
MD5:	DB2EDF1465946C06BD95C71A1E13AE64
SHA1:	FB4F3ECE9ECECEBBC6CA2A592A15FB9C1FDFB811
SHA-256:	FBAF22CE6E16DE174CED8CB5EA3098CCA1C3426A2111FF33BD3E64DA64ED67AB
SHA-512:	4E0CF00BAEF1757548DEB17BBE1AF55770A0A0F7351779EF55C7DEFA6D112D0227B8865C2C22E0EC62E6E2F1C8E1632A2D0CE6828D25C5ABBF143C990116F632
Malicious:	false
Preview:	{.. "app_description": {.. "message": "..... Chrome".. },.. "app_name": {.. "message": "..... Chrome".. },.. "crawl_app_unavailable": {.. "message": ".....".. },.. "crawl_connect_to_network": {.. "message": ".....".. },.. "iap_unavailable": {.. "message": "..... .. Chrome".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed".. },.. "please_sign_in": {.. "message": "..... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir1828_1251794979\CRX_INSTALL_locales\sk\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.640777810668463
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34ORO+dgmmCO8ZpU34yH7u2Z03OyZnLAOfTYCUAi0D:1HEI4G8WYpetPmD8ZpcH7aOGAOfzUeD
MD5:	8DF215D1EFBDABB175CCDD68ED8DCB0A
SHA1:	2B374462137A38589A73FDD00A84CBDC7E50F9F4
SHA-256:	7FA16AF97E6CFC52EC6008EB679D3F30E7E0C24F9EF2D18A9228EAF4DED9D63B
SHA-512:	C0E62334BDAEB4731800D183B59F2FCFE285F0C7153EC99641FD84F2F2DCFE47D21E73F3D28B1240340453C5668EB0AFFBE087AAB62F1C88CD2A40CC44E59D

Malicious:	false
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. }... "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. }... "crawl_app_unavailable": {.. "message": "Aplik.cia moment.lne nie je dostupn..".. }... "crawl_connect_to_network": {.. "message": "Pripojte sa k sieti..".. }... "iap_unavailable": {.. "message": "Platby v aplik.cii moment.lne nie s. k dispoz.cii..".. }... "jwt_retrieve_failed": {.. "message": "The transaction could not be completed..".. }... "please_sign_in": {.. "message": "Prihl.ste sa do prehliada.a Chrome..".. }...}..

Static File Info	
General	
File type:	Microsoft Excel 2007+
Entropy (8bit):	7.991276862113107
TrID:	- Excel Microsoft Office Open XML Format document (40004/1) 83.33% - ZIP compressed archive (8000/1) 16.67%
File name:	Invoice#0036473 .xlsx
File size:	935361
MD5:	c93e6dcf32928e1da7346b6ca3a1dc85
SHA1:	b90d66412b4d6669a175fd30e32bbe44428bd245
SHA256:	3ffe69c9e2e2f8a350f7d2ff6e64acf8cfbf390489807b81cf8e4eec87d4047
SHA512:	285b0a357b59b8c0cfc0bcbd91706e12e90e3d4f56b516b05ba745ec3b036b217c9029a250269c947c40108d3d9431ab5b26a54da7df88b56ffbf2ac8d9fc533
SSDEEP:	24576:4rQU57GpJk69mCNDPCBPY+bikHII5Bqn13dhW7:/y7jCIPsDJ55B67W7
TLSH:	C21533D9983763EDE23F9CB1126BA700742474871970C4D14ECAA9C1FE94EF794BB12
File Content Preview:	PK.....!.."p.....[Content_Types].xml ... (.....)

File Icon	
	
Icon Hash:	74ecd0d2d6d6d0dc

Network Behavior	
Network Port Distribution	
 Total Packets: 84 53 (DNS) 443 (HTTPS)	

TCP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 1, 2022 16:30:00.328988075 CEST	49807	443	192.168.2.3	142.251.36.205
Jul 1, 2022 16:30:00.329052925 CEST	443	49807	142.251.36.205	192.168.2.3
Jul 1, 2022 16:30:00.329164982 CEST	49807	443	192.168.2.3	142.251.36.205
Jul 1, 2022 16:30:00.330379963 CEST	49807	443	192.168.2.3	142.251.36.205

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 1, 2022 16:30:00.330415010 CEST	443	49807	142.251.36.205	192.168.2.3
Jul 1, 2022 16:30:00.335041046 CEST	49808	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:00.335093975 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.335808039 CEST	49809	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:00.335834980 CEST	49808	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:00.335867882 CEST	443	49809	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.336314917 CEST	49808	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:00.336347103 CEST	49809	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:00.336357117 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.336652040 CEST	49809	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:00.336682081 CEST	443	49809	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.341959000 CEST	49810	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:00.342017889 CEST	443	49810	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:00.342170000 CEST	49810	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:00.342396021 CEST	49810	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:00.342422962 CEST	443	49810	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:00.414232969 CEST	443	49807	142.251.36.205	192.168.2.3
Jul 1, 2022 16:30:00.416224003 CEST	443	49810	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:00.426099062 CEST	49810	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:00.426157951 CEST	443	49810	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:00.426302910 CEST	49807	443	192.168.2.3	142.251.36.205
Jul 1, 2022 16:30:00.426342010 CEST	443	49807	142.251.36.205	192.168.2.3
Jul 1, 2022 16:30:00.427175045 CEST	443	49810	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:00.427288055 CEST	49810	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:00.427664042 CEST	443	49807	142.251.36.205	192.168.2.3
Jul 1, 2022 16:30:00.427747965 CEST	49807	443	192.168.2.3	142.251.36.205
Jul 1, 2022 16:30:00.429404974 CEST	443	49810	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:00.429486990 CEST	49810	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:00.621412039 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.625559092 CEST	49808	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:00.625603914 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.628547907 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.628669977 CEST	49808	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:00.632052898 CEST	443	49809	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.635247946 CEST	49809	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:00.635298014 CEST	443	49809	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.636537075 CEST	443	49809	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.636622906 CEST	49809	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:00.649446011 CEST	49807	443	192.168.2.3	142.251.36.205
Jul 1, 2022 16:30:00.649571896 CEST	49810	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:00.649645090 CEST	49808	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:00.649796963 CEST	443	49807	142.251.36.205	192.168.2.3
Jul 1, 2022 16:30:00.650000095 CEST	443	49810	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:00.650007963 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.650238991 CEST	49809	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:00.650418997 CEST	443	49809	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.650571108 CEST	49807	443	192.168.2.3	142.251.36.205
Jul 1, 2022 16:30:00.650609016 CEST	443	49807	142.251.36.205	192.168.2.3
Jul 1, 2022 16:30:00.650679111 CEST	49810	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:00.650713921 CEST	443	49810	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:00.650985956 CEST	49808	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:00.651016951 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.687513113 CEST	443	49810	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:00.687654972 CEST	443	49810	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:00.687774897 CEST	49810	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:00.699531078 CEST	49810	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:00.699584961 CEST	443	49810	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:00.716790915 CEST	443	49807	142.251.36.205	192.168.2.3
Jul 1, 2022 16:30:00.716949940 CEST	49807	443	192.168.2.3	142.251.36.205

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 1, 2022 16:30:00.716993093 CEST	443	49807	142.251.36.205	192.168.2.3
Jul 1, 2022 16:30:00.717072964 CEST	443	49807	142.251.36.205	192.168.2.3
Jul 1, 2022 16:30:00.717159986 CEST	49807	443	192.168.2.3	142.251.36.205
Jul 1, 2022 16:30:00.723100901 CEST	49807	443	192.168.2.3	142.251.36.205
Jul 1, 2022 16:30:00.723145962 CEST	443	49807	142.251.36.205	192.168.2.3
Jul 1, 2022 16:30:00.736763954 CEST	49808	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:00.856509924 CEST	443	49809	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.856594086 CEST	49809	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:00.883204937 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.883279085 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.883300066 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.883397102 CEST	49808	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:00.883409977 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.883447886 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:00.883491993 CEST	49808	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:00.936781883 CEST	49808	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:01.015044928 CEST	49809	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:01.018090963 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:01.018127918 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:01.018213987 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:01.018222094 CEST	49808	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:01.018265963 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:01.018269062 CEST	49808	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:01.018286943 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:01.018287897 CEST	49808	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:01.018352032 CEST	49808	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:01.018371105 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:01.018441916 CEST	49808	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:01.018507004 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:01.018589020 CEST	49808	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:01.022614002 CEST	49808	443	192.168.2.3	69.49.244.155
Jul 1, 2022 16:30:01.022644997 CEST	443	49808	69.49.244.155	192.168.2.3
Jul 1, 2022 16:30:01.045535088 CEST	49817	443	192.168.2.3	104.18.10.207
Jul 1, 2022 16:30:01.045576096 CEST	443	49817	104.18.10.207	192.168.2.3
Jul 1, 2022 16:30:01.045758963 CEST	49817	443	192.168.2.3	104.18.10.207
Jul 1, 2022 16:30:01.045938969 CEST	49817	443	192.168.2.3	104.18.10.207
Jul 1, 2022 16:30:01.045964956 CEST	443	49817	104.18.10.207	192.168.2.3

UDP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 1, 2022 16:30:00.294583082 CEST	50152	53	192.168.2.3	8.8.8.8
Jul 1, 2022 16:30:00.312707901 CEST	50450	53	192.168.2.3	8.8.8.8
Jul 1, 2022 16:30:00.314197063 CEST	52427	53	192.168.2.3	8.8.8.8
Jul 1, 2022 16:30:00.322047949 CEST	53	50152	8.8.8.8	192.168.2.3
Jul 1, 2022 16:30:00.333883047 CEST	53	50450	8.8.8.8	192.168.2.3
Jul 1, 2022 16:30:00.340058088 CEST	53	52427	8.8.8.8	192.168.2.3
Jul 1, 2022 16:30:00.990426064 CEST	54960	53	192.168.2.3	8.8.8.8
Jul 1, 2022 16:30:00.993556023 CEST	64624	53	192.168.2.3	8.8.8.8
Jul 1, 2022 16:30:01.014316082 CEST	51779	53	192.168.2.3	8.8.8.8
Jul 1, 2022 16:30:01.015187979 CEST	53	64624	8.8.8.8	192.168.2.3
Jul 1, 2022 16:30:01.337953091 CEST	54205	53	192.168.2.3	8.8.8.8
Jul 1, 2022 16:30:01.338164091 CEST	62756	53	192.168.2.3	8.8.8.8
Jul 1, 2022 16:30:01.357351065 CEST	53	62756	8.8.8.8	192.168.2.3
Jul 1, 2022 16:30:01.359735966 CEST	58497	53	192.168.2.3	8.8.8.8
Jul 1, 2022 16:30:01.359962940 CEST	62701	53	192.168.2.3	8.8.8.8
Jul 1, 2022 16:30:01.381726980 CEST	53	58497	8.8.8.8	192.168.2.3
Jul 1, 2022 16:30:01.382255077 CEST	53	62701	8.8.8.8	192.168.2.3
Jul 1, 2022 16:30:01.636451006 CEST	53524	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jul 1, 2022 16:30:01.658387899 CEST	53	53524	8.8.8.8	192.168.2.3
Jul 1, 2022 16:30:02.326417923 CEST	61555	53	192.168.2.3	8.8.8.8
Jul 1, 2022 16:30:02.357074976 CEST	53	61555	8.8.8.8	192.168.2.3
Jul 1, 2022 16:30:04.015841007 CEST	64433	53	192.168.2.3	8.8.8.8
Jul 1, 2022 16:30:04.043605089 CEST	53	64433	8.8.8.8	192.168.2.3
Jul 1, 2022 16:30:04.103030920 CEST	64435	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:04.113660097 CEST	62547	53	192.168.2.3	8.8.8.8
Jul 1, 2022 16:30:04.120584965 CEST	54096	53	192.168.2.3	8.8.8.8
Jul 1, 2022 16:30:04.135622025 CEST	53	62547	8.8.8.8	192.168.2.3
Jul 1, 2022 16:30:04.137655020 CEST	53	54096	8.8.8.8	192.168.2.3
Jul 1, 2022 16:30:04.143904924 CEST	443	64435	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:04.148303986 CEST	64435	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:04.188908100 CEST	443	64435	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:04.188956022 CEST	443	64435	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:04.188994884 CEST	443	64435	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:04.189034939 CEST	443	64435	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:04.189313889 CEST	64435	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:04.191221952 CEST	64435	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:04.210666895 CEST	49230	53	192.168.2.3	8.8.8.8
Jul 1, 2022 16:30:04.230278969 CEST	64435	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:04.230623007 CEST	64435	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:04.231647015 CEST	53	49230	8.8.8.8	192.168.2.3
Jul 1, 2022 16:30:04.276401043 CEST	443	64435	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:04.283129930 CEST	443	64435	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:04.284688950 CEST	443	64435	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:04.285279036 CEST	64435	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:04.294152975 CEST	443	64435	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:04.294190884 CEST	443	64435	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:04.294219971 CEST	443	64435	142.251.36.238	192.168.2.3
Jul 1, 2022 16:30:04.294967890 CEST	64435	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:04.320013046 CEST	64435	443	192.168.2.3	142.251.36.238
Jul 1, 2022 16:30:37.462620974 CEST	51994	53	192.168.2.3	8.8.8.8
Jul 1, 2022 16:30:37.496638060 CEST	53	51994	8.8.8.8	192.168.2.3
Jul 1, 2022 16:30:39.002104044 CEST	51658	53	192.168.2.3	8.8.8.8
Jul 1, 2022 16:30:39.020740986 CEST	53	51658	8.8.8.8	192.168.2.3
Jul 1, 2022 16:30:44.534595013 CEST	58951	443	192.168.2.3	172.217.16.161
Jul 1, 2022 16:30:44.575727940 CEST	443	58951	172.217.16.161	192.168.2.3
Jul 1, 2022 16:30:44.709163904 CEST	58951	443	192.168.2.3	172.217.16.161
Jul 1, 2022 16:30:44.749865055 CEST	443	58951	172.217.16.161	192.168.2.3
Jul 1, 2022 16:30:44.749906063 CEST	443	58951	172.217.16.161	192.168.2.3
Jul 1, 2022 16:30:44.749927044 CEST	443	58951	172.217.16.161	192.168.2.3
Jul 1, 2022 16:30:44.749948025 CEST	443	58951	172.217.16.161	192.168.2.3
Jul 1, 2022 16:30:44.750293970 CEST	58951	443	192.168.2.3	172.217.16.161
Jul 1, 2022 16:30:44.751456022 CEST	58951	443	192.168.2.3	172.217.16.161
Jul 1, 2022 16:30:44.821082115 CEST	58951	443	192.168.2.3	172.217.16.161
Jul 1, 2022 16:30:44.821309090 CEST	58951	443	192.168.2.3	172.217.16.161
Jul 1, 2022 16:30:44.867759943 CEST	443	58951	172.217.16.161	192.168.2.3
Jul 1, 2022 16:30:44.873756886 CEST	443	58951	172.217.16.161	192.168.2.3
Jul 1, 2022 16:30:44.876708984 CEST	443	58951	172.217.16.161	192.168.2.3
Jul 1, 2022 16:30:44.877312899 CEST	58951	443	192.168.2.3	172.217.16.161
Jul 1, 2022 16:30:44.883070946 CEST	443	58951	172.217.16.161	192.168.2.3
Jul 1, 2022 16:30:44.888621092 CEST	58951	443	192.168.2.3	172.217.16.161
Jul 1, 2022 16:30:44.932451010 CEST	443	58951	172.217.16.161	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 1, 2022 16:30:00.294583082 CEST	192.168.2.3	8.8.8.8	0xe338	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 1, 2022 16:30:00.312707901 CEST	192.168.2.3	8.8.8.8	0xb455	Standard query (0)	eyecandyla shcompany.com	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:00.314197063 CEST	192.168.2.3	8.8.8.8	0x481f	Standard query (0)	clients2.g oogle.com	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:00.990426064 CEST	192.168.2.3	8.8.8.8	0xb975	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:00.993556023 CEST	192.168.2.3	8.8.8.8	0xb92e	Standard query (0)	maxcdnn.boo tstrapcdn.com	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:01.014316082 CEST	192.168.2.3	8.8.8.8	0x76b0	Standard query (0)	kit.fontaw esome.com	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:01.337953091 CEST	192.168.2.3	8.8.8.8	0xecde	Standard query (0)	ka-f.fonta wesome.com	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:01.338164091 CEST	192.168.2.3	8.8.8.8	0x7814	Standard query (0)	cdnjs.clou dflare.com	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:01.359735966 CEST	192.168.2.3	8.8.8.8	0x39c4	Standard query (0)	stackpath. bootstrapc dn.com	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:01.359962940 CEST	192.168.2.3	8.8.8.8	0xa982	Standard query (0)	cdn.iconsc out.com	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:01.636451006 CEST	192.168.2.3	8.8.8.8	0xee9b	Standard query (0)	cdn.pixabay.com	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:02.326417923 CEST	192.168.2.3	8.8.8.8	0xc0f7	Standard query (0)	lh3.google usercontent.com	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:04.015841007 CEST	192.168.2.3	8.8.8.8	0xd9fd	Standard query (0)	lh3.google usercontent.com	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:04.113660097 CEST	192.168.2.3	8.8.8.8	0x8b7d	Standard query (0)	cdn.iconsc out.com	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:04.120584965 CEST	192.168.2.3	8.8.8.8	0x931f	Standard query (0)	eyecandyla shcompany.com	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:04.210666895 CEST	192.168.2.3	8.8.8.8	0x6c8b	Standard query (0)	cdn.pixabay.com	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:37.462620974 CEST	192.168.2.3	8.8.8.8	0xdb05	Standard query (0)	eyecandyla shcompany.com	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:39.002104044 CEST	192.168.2.3	8.8.8.8	0x415a	Standard query (0)	eyecandyla shcompany.com	A (IP address)	IN (0x0001)

DNS Answers									
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 1, 2022 16:30:00.322047949 CEST	8.8.8.8	192.168.2.3	0xe338	No error (0)	accounts.g oogle.com		142.251.36.205	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:00.333883047 CEST	8.8.8.8	192.168.2.3	0xb455	No error (0)	eyecandyla shcompany.com		69.49.244.155	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:00.340058088 CEST	8.8.8.8	192.168.2.3	0x481f	No error (0)	clients2.g oogle.com	clients.l.google.co m		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 16:30:00.340058088 CEST	8.8.8.8	192.168.2.3	0x481f	No error (0)	clients.l. google.com		142.251.36.238	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:01.007193089 CEST	8.8.8.8	192.168.2.3	0xb975	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcd n.net		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 16:30:01.015187979 CEST	8.8.8.8	192.168.2.3	0xb92e	No error (0)	maxcdnn.boo tstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:01.015187979 CEST	8.8.8.8	192.168.2.3	0xb92e	No error (0)	maxcdnn.boo tstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:01.032870054 CEST	8.8.8.8	192.168.2.3	0x76b0	No error (0)	kit.fontaw esome.com	kit.fontawesome.c om.cdn.cloudflare. net		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 16:30:01.266529083 CEST	8.8.8.8	192.168.2.3	0xdebe	No error (0)	gstaticads sl.l.google.com		142.251.36.227	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:01.357281923 CEST	8.8.8.8	192.168.2.3	0xecde	No error (0)	ka-f.fonta wesome.com	ka-f.fontawesome.co m.cdn.cloudflare.n et		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 16:30:01.357351065 CEST	8.8.8.8	192.168.2.3	0x7814	No error (0)	cdnjs.clou dflare.com		104.17.24.14	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:01.357351065 CEST	8.8.8.8	192.168.2.3	0x7814	No error (0)	cdnjs.clou dflare.com		104.17.25.14	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:01.381726980 CEST	8.8.8.8	192.168.2.3	0x39c4	No error (0)	stackpath. bootstrapc dn.com		104.18.10.207	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 1, 2022 16:30:01.381726980 CEST	8.8.8.8	192.168.2.3	0x39c4	No error (0)	stackpath. bootstrapc dn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:01.382255077 CEST	8.8.8.8	192.168.2.3	0xa982	No error (0)	cdn.icons out.com		104.18.28.243	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:01.382255077 CEST	8.8.8.8	192.168.2.3	0xa982	No error (0)	cdn.icons out.com		104.18.29.243	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:01.658387899 CEST	8.8.8.8	192.168.2.3	0xee9b	No error (0)	cdn.pixabay.com		172.64.150.12	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:01.658387899 CEST	8.8.8.8	192.168.2.3	0xee9b	No error (0)	cdn.pixabay.com		104.18.37.244	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:02.357074976 CEST	8.8.8.8	192.168.2.3	0xc0f7	No error (0)	lh3.google usercontent.com	googlehosted.l.goo gleusercontent.co m		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 16:30:02.357074976 CEST	8.8.8.8	192.168.2.3	0xc0f7	No error (0)	googlehost ed.l.googl euserconte nt.com		172.217.16.161	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:04.043605089 CEST	8.8.8.8	192.168.2.3	0xd9fd	No error (0)	lh3.google usercontent.com	googlehosted.l.goo gleusercontent.co m		CNAME (Canonical name)	IN (0x0001)
Jul 1, 2022 16:30:04.043605089 CEST	8.8.8.8	192.168.2.3	0xd9fd	No error (0)	googlehost ed.l.googl euserconte nt.com		172.217.16.161	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:04.135622025 CEST	8.8.8.8	192.168.2.3	0x8b7d	No error (0)	cdn.icons out.com		104.18.29.243	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:04.135622025 CEST	8.8.8.8	192.168.2.3	0x8b7d	No error (0)	cdn.icons out.com		104.18.28.243	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:04.137655020 CEST	8.8.8.8	192.168.2.3	0x931f	No error (0)	eyecandyla shcompany.com		69.49.244.155	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:04.231647015 CEST	8.8.8.8	192.168.2.3	0x6c8b	No error (0)	cdn.pixabay.com		104.18.37.244	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:04.231647015 CEST	8.8.8.8	192.168.2.3	0x6c8b	No error (0)	cdn.pixabay.com		172.64.150.12	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:37.496638060 CEST	8.8.8.8	192.168.2.3	0xdb05	No error (0)	eyecandyla shcompany.com		69.49.244.155	A (IP address)	IN (0x0001)
Jul 1, 2022 16:30:39.020740986 CEST	8.8.8.8	192.168.2.3	0x415a	No error (0)	eyecandyla shcompany.com		69.49.244.155	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- eyecandylashcompany.com
- https:
 - maxcdn.bootstrapcdn.com
 - cdnjs.cloudflare.com
 - stackpath.bootstrapcdn.com
 - cdn.iconscout.com
 - cdn.pixabay.com
 - lh3.googleusercontent.com

HTTPS Proxied Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49807	142.251.36.205	443	C:\Program Files\Google\Chrome\Application\chrome.exe
Timestamp	kBytes transferred	Direction	Data		

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:00 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
2022-07-01 14:30:00 UTC	0	OUT	Data Raw: 20 Data Ascii:
2022-07-01 14:30:00 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, 01 Jul 2022 14:30:00 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Cross-Origin-Opener-Policy: same-origin; report-to="IdentityListAccountsHttp" Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/_/IdentityListAccountsHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-knviCwJOBAtNlkt3gtY_A' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-knviCwJOBAtNlkt3gtY_A' '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 Report-To: {"group":"IdentityListAccountsHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/identityListAccountsHttp/external"}]} 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=*\nServer: ESF\nX-XSS-Protection: 0\nAlt-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"\nAccept-Ranges: none\nVary: Accept-Encoding\nConnection: close\nTransfer-Encoding: chunked
2022-07-01 14:30:00 UTC	5	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",[]]
2022-07-01 14:30:00 UTC	5	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	49810	142.251.36.238	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:00 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%3Dnmmhkkegcagdldgiimedpiccmgmieda%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: nmmhkkegcagdldgiimedpiccmgmieda,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

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:00 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-Rzx6bD_OtREeMnL4lu0ZAg' 'unsafe-inline' 'strict-dynamic' http s: 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, 01 Jul 2022 14:30:00 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5660 X-Daystart: 27000 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"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-07-01 14:30:00 UTC	2	IN	Data Raw: 33 31 61 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 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 36 30 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 32 37 30 30 30 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: 31a<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" p rotocol="2.0" server="prod"><daystart elapsed_days="5660" elapsed_seconds="27000"/><app appid="nmhkhkgeccagldd giimedpiccmgmieda" cohort="1.:" cohortname=""
2022-07-01 14:30:00 UTC	3	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: mhhkgeccaglddgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c54 50122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" p roTECTED="0" size="248531" status="ok" version="1.0.0.6"/></app><ap
2022-07-01 14:30:00 UTC	3	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	49824	69.49.244.155	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	410	OUT	GET /payment/frontend_paper_lantern/images/gmail.png HTTP/1.1 Host: eyecandylashcompany.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://eyecandylashcompany.com/payment/frontend_paper_lantern/index.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-07-01 14:30:01 UTC	419	IN	HTTP/1.1 404 Not Found Date: Fri, 01 Jul 2022 14:30:00 GMT Server: Apache Content-Length: 315 Connection: close Content-Type: text/html; charset=iso-8859-1
2022-07-01 14:30:01 UTC	419	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body><h1>Not Found</h1><p>The requested URL was not found on this server.</p><p>Additionally, a 404 Not Found error was encountered while trying to use

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	425	IN	Data Raw: 49 38 9d 9c 4e 90 9d 38 93 a1 93 a1 9d 68 d6 7f ac 73 9d e9 d6 69 54 25 c9 5a 51 d1 24 87 8c 98 6f 16 f6 9e 0f 3b f2 e9 b4 bc de b8 c2 6f 02 2c 26 5b b6 5d 59 ac d7 e8 5b 4c 4d 88 1e 37 4d 43 5b 58 8e 85 73 eb 16 c7 32 6b 1e 61 83 e9 7e 39 c3 a6 a6 80 33 f7 8f a1 eb fc 57 d1 3a 73 ed 45 cf ec 6f 39 79 1d a3 47 3d d2 d6 55 a8 b0 49 6e ce 56 a5 44 b3 4b 3e c9 65 ac 88 af 60 24 ab 2a 71 38 1e 22 eb f8 fd 33 9b 37 3d aa d7 60 65 63 f5 59 f5 c5 75 59 78 3e 8e 1f 51 4b 1b 63 a7 2c 3f 9d be a9 e5 f4 f1 7f 68 ea c4 53 d2 ad 63 48 19 39 28 c4 01 68 87 2e ad 4a 85 9b 2c a1 82 09 6f 0e da e9 8e 12 4b 92 09 c0 8d 56 5c de 7f 4b 2b 16 80 6d d4 ce a3 31 c5 2d 59 cb 35 6a d1 14 09 12 05 84 58 16 a3 35 25 09 48 5b 23 22 84 f5 09 42 5a c3 a4 c8 82 68 4b c9 78 e7 d1 3f 39 Data Ascii: l8N8hsiT%ZQ\$o;o,&[]Y[LM7MC[Xs2ka~93AW:sEo9yG=UlnVDK>e`\$*q8"37=``ecYuYx>QKc,?hScH9(h.J,oKV\K+m1-Y5jX5%H[#BZhKx?9
2022-07-01 14:30:01 UTC	426	IN	Data Raw: ae 6f cf e9 85 b1 5d c7 56 91 cd 9a 5d 6c cb f3 56 a6 35 61 4f 5a 45 c8 42 36 02 f6 75 f8 23 dc ad ac c2 f5 46 5b cf 5e f5 cc 5e ca 93 82 c0 ec b9 2c 5a 33 b8 38 0a d1 14 b9 a5 b4 4a ce a9 ac 24 c5 86 d1 75 39 b6 ea e1 6a 7a 71 76 19 dd 0d 02 bd 25 09 d4 03 60 11 43 ae e0 bb 2f 47 0b 31 84 3a f2 2c 40 30 f0 1a a2 bd 40 25 ca f5 eb 16 05 5a a2 de cd b2 a3 27 4c 70 5d a1 56 9a 42 60 b0 a3 af a1 4d 29 46 da 5a 54 f5 eb 18 ed 64 38 a3 62 c3 20 91 46 a7 60 0c ba 26 ca b4 1a 9d c6 4c b5 6c 19 d0 e4 d5 ac b3 87 b5 2d d1 41 f3 98 f5 ec ee 3c ff 00 d0 79 c3 73 37 d0 89 18 bd 27 9d f2 d9 d4 69 ee d5 97 2c 9a 24 b2 85 9b 8b 3a 0d 4b 35 35 9a 4d 75 ac a7 3b 52 00 5b 25 cd 8d da f6 b3 b9 19 59 c6 a0 49 3c b5 40 a8 ef 24 8b 4e c9 d5 56 10 4f 62 4a e5 84 73 6b e6 e8 54 d6 Data Ascii: oJv]V5aOZEB6u#F[^,Z38J\$u9dzqv%`C/G1:,@0@%Z`Lp]VB`M)FZTd8b F`&LI-A<ys?i,\$:K55Mu;R[%YI<@ \$NVOBJskT
2022-07-01 14:30:01 UTC	427	IN	Data Raw: a6 90 40 a6 62 c1 2a 9b 22 47 3b 4a c1 cb 9d a4 75 d9 37 ec ad 78 79 d5 e9 2d f3 fe a9 58 2e 77 71 c0 47 7d c6 79 da 53 88 a7 ce a8 c9 9e c5 28 92 08 48 4f 3b 94 e4 f9 b0 49 c7 33 d9 ce 87 62 33 cd ae db 02 de 71 e8 f4 74 b5 29 cb 46 30 0b 4a de 75 1b 55 2d 66 cc 16 94 50 b4 1b 15 5a be b1 4a 04 d4 24 60 c7 76 91 90 1b 82 ac a0 e9 3e f3 98 fa 81 07 64 20 2e 0e 99 91 83 76 52 d2 8e 8d a3 0e 5d 15 55 c5 b3 a9 9d 62 6b 56 a5 cc 1e b4 0c f5 7d 8a 04 b0 45 a6 4b 44 80 42 c6 75 23 82 36 5f 3d 38 66 db 82 79 69 54 d3 ad a8 51 41 11 bd 4a eb 5d 36 90 74 73 b1 f4 1c 76 84 d7 49 48 0 3 b2 70 a9 77 35 b7 28 5b b9 ab cb ea 72 0b 2b 58 ad 35 b5 3c a9 66 bd 09 03 af 3a 56 03 95 be 50 d1 a7 78 29 99 b9 f4 91 80 49 ae c7 73 0f a3 e5 d4 2f 60 75 43 3f 50 32 e5 de ab 42 cd Data Ascii: @b""G;Ju7xy-X.wqGjyS(HO;l3b3qt)F0JuU-fPZJ\$`v>d .vRjUbkVjEKDBu#6_~8fiyTQAJ]6tsvlHpw5([r+X5<f:VPxj)ls/'uC?P2B
2022-07-01 14:30:01 UTC	429	IN	Data Raw: cc 22 b3 19 6b 4e e5 94 ce ab b0 05 cd 7b f5 13 4f d5 b9 c0 76 e1 b5 e7 fd 96 45 9d 2e 5f 8a 7a c6 a7 8f fd 09 f3 bf 6d 5e e3 8c a1 73 e8 07 2c 27 41 04 e2 9a a9 46 ee 6e 37 95 52 dd 59 6a 52 bf 5c cb cf de 0d ce 71 65 46 e6 cb d1 bd ac c8 84 dc cd a8 78 db cb a9 92 cc a0 26 32 29 b9 6c 99 04 b7 5e e6 20 3a b4 34 af 02 ce 75 b4 71 fa e0 e3 ae 09 74 ad e0 68 5b a9 73 39 f9 f4 d3 2e 7d ac 6f 46 e5 2b d9 b2 13 80 a5 52 c5 4d e0 13 8c fa 73 24 dc 8b 12 ad 18 8d c7 b5 c6 82 be 9b 4b 97 6a c3 d6 65 6e 8b 26 c8 ca c5 62 95 3b 31 de 71 2b eb d4 d6 73 0d 67 3b 50 f4 6d 06 ca e8 af 72 19 1a 20 dc 8e 09 15 10 79 ba 85 ca e5 72 5a 8c 54 21 91 08 da 14 a1 6b 4f 55 ca 45 08 d5 83 1a 8f 9c f2 de 54 23 66 88 e9 11 6e 12 a5 8c d7 23 cd 7a 9a 7c 46 56 e7 a7 57 f3 75 be 7e Data Ascii: "kN{OvE,_zm^As,AFn7RYjRlqeFx&2)l^ :4uqth[s9,.joF+RMs\$Kjen&b;1q+sg;Pmr yrZT!kOUEt#fnzjFVWu~
2022-07-01 14:30:01 UTC	430	IN	Data Raw: 8f 62 ab 45 eb 99 f7 b3 a2 c8 e1 88 ed e4 75 9a ce 85 5e ed bd 3c 3c e6 b7 a7 a3 c8 6b 7b 32 97 c3 ab 7b d3 cb f3 fd 1f a2 eb cb f3 e4 bd d6 ac be 21 1f 6a a7 1e 35 5f d8 29 57 94 8b d3 a9 59 e7 ad da d5 b3 95 1f 4b 9e 64 ae fb af b3 c3 7e 86 6e 9f 59 71 5a 92 06 36 14 a3 79 a2 2a 4d 4c 9d 91 99 e2 3a 8a 24 a0 89 b8 dc 94 46 0a f9 64 3d 77 31 8e d5 9d e3 d3 93 a6 78 45 17 a0 4d 75 78 b1 a7 e0 fa 1d 37 a9 e6 f9 4f b3 c3 d2 78 8c 27 ac 8e c5 ab f8 dc b4 e9 37 2e 87 cc b6 5b 33 6c da 70 b3 00 33 ab d1 a4 74 3d 4b 08 a4 5b 33 aa e9 52 b2 d1 6a da 87 89 84 b1 69 0a c3 df d8 f4 2a ad a2 95 4e 41 5a 96 5e ab 25 80 08 33 43 ad 2a f8 db 85 3e 76 10 9e a6 6a ac 3a b3 56 21 9c 22 e0 ab 22 70 80 ec 20 1d ec 1c 9d 23 45 a2 4e 60 9a aa 57 f3 ec 2f 53 c5 5e b3 73 6e a6 Data Ascii: bEu<<<[2lj5_]WYKd~nYqZ6y*ML:\$Fd=w1xE慕7Ox'7.[3lp3t=K[3Rji*NAZ`%3C*>vj:V!""p #EN`W/S^sn
2022-07-01 14:30:01 UTC	431	IN	Data Raw: 2b 7c b5 6b 52 d5 df 3d 60 3f 3b ac 8c f9 4f bc eb ce 1e a1 9b c2 77 5e 90 73 ce 0f d7 cc e4 36 ba 5a da c9 a1 57 9b b3 b1 e6 b5 74 cc ae 37 a3 db 38 3f 3f fa 1f ce f3 af 32 8d 91 70 f4 c6 cd 53 2e bd cd bb b8 d9 86 46 4a 48 b5 16 fd 12 30 33 0a 65 87 19 08 40 95 88 c1 c6 82 af 6a be 1f 52 cd 7d 2e 9c bd 4f c6 7e 97 f0 0b 9c 38 58 58 d5 48 db 95 94 09 3a f6 1d e2 cb 6a c5 69 e6 d9 95 43 4a ff 00 41 7c fd f4 4f 5e 6a 51 97 5e 52 76 71 3b 3c ae 9a 30 45 19 2a 49 95 dd 9e 47 49 e1 95 6e 5f 3b eb 79 ce 46 af 9b b5 cc ab 72 e1 d6 aa b6 d2 d6 21 63 11 69 0d 49 2a a6 0e 41 cc 71 d8 ae 82 89 ab ac 3d 3b cc ba 0e dc f6 ee 68 79 7f af cd dc ef fc 99 e9 5b cf b5 b5 2b 61 07 20 9f 3a 40 6f c3 bb 0e 42 b1 88 17 b9 94 5a 56 8b 4f 00 53 77 09 a3 99 7b 3a bf 63 01 66 ec Data Ascii: +lK=R`?:Ow"s6ZWt78??2pS.FJH03e@jRj;.O~8XXH:jiCJA O`jQ`Rvq;<0E`IGln_yfRcil`Aq=:hy[+a :@oBZVOSw[:cf
2022-07-01 14:30:01 UTC	433	IN	Data Raw: e3 c0 74 3d f9 fb 72 e4 35 b7 9f a7 3a e6 22 b8 00 ed 0e b3 4a 5a f9 57 bf 0a 7c 3a 74 33 a7 62 bc bb 80 f7 ef 08 e5 d6 9d 83 2c 6e 06 78 c0 e5 19 0c 8d 0a ee 3d 37 cf bd 07 d1 c1 3a 5b c3 bb 50 97 41 53 b8 70 18 5d df 01 e4 f4 e8 14 10 f3 f5 b0 f0 3c a3 92 51 39 b4 e5 91 22 c8 d1 94 15 56 38 0a 19 da b3 cd 24 97 4e 49 24 24 ce 3b c5 cf 4a d0 ad 6b e7 7b 98 25 8e 37 56 49 a9 92 85 9e d2 5e 43 af fa 1e 18 42 4d d3 3f 32 07 4e af 1e d5 aa dd 8d cd 36 b7 2b 2a 0f 53 d7 75 39 1f 63 2b ef 32 2b 92 c6 61 d4 8b ab 1e a4 bd 33 73 db d6 19 40 12 d8 18 27 62 4f 0a 95 76 8c 55 0d d0 ac 14 a5 2d 6a d7 43 19 e2 d1 a7 8d 0c 71 1c a5 03 40 9e da e9 b7 94 9d 6a 36 56 b6 5c 9f 33 5e a7 a9 cf ac cd 67 bc cd f3 81 7a 3d 5b 3c f8 7d c5 5b 38 b9 74 d5 Data Ascii: t=r5:"JZWj:t3b,nx=7:[PASP]<Q9"V8(yy\$Nl\$\$.Jk(%7VI^CBM?2N6++Su9c+2+a3s@'bOvU-jCq@j6Vl3`gz=[<]8t
2022-07-01 14:30:01 UTC	434	IN	Data Raw: f1 89 c8 88 3c a0 11 41 a0 8c 9c 84 6c b9 50 b2 ae 46 a5 dc d0 30 c9 ce ce ba 1d 5e 2a cc bd b7 33 af 7f 78 a5 85 b7 62 5e 1b 5f 2e 1c f7 1b 12 a4 59 62 5c b0 1d 9b 97 a6 52 4a 92 48 49 21 24 a1 d9 88 55 ec 00 f9 5e d5 4d 3e 7b ed bb 4e 47 ac ce 54 85 62 21 14 50 0c 50 92 70 31 60 61 65 25 5b d9 c9 af b9 8b b1 b9 75 87 0d 42 ce b4 8b 0f 5d 17 1e ac cb 08 33 26 a2 e4 88 31 13 69 00 20 9e 46 3f 3b d2 e0 f7 c8 4f 5e df 4c d8 b3 58 d7 37 0f 4e c4 58 50 9c a4 98 67 2c dd 91 28 ba 86 8b a2 10 90 75 25 c1 f7 15 73 7c 48 d9 c0 f1 7a af 42 a2 2d b4 61 29 1a 10 b2 c5 cc 7d db 3e 81 82 5d f8 24 92 ba 07 0a 7a 13 c6 21 27 c6 76 52 bb 3a 38 ae 13 d9 bc 77 cd df 4a 75 6d 79 7d 02 29 26 4e c0 9e 43 33 10 6a d6 c1 14 31 f7 32 36 a5 e7 9d ff 00 01 ed f3 33 b2 eb cd 24 84 Data Ascii: <AIPF0**3xb^_.YbIRJHI\$U^M>[NGTbIPpp1`ae%[uBj3&i F?;O^LX7NXPg,(u%sjHzB-a)>]\$z!vR:8wJu myj)&NC3j1263\$
2022-07-01 14:30:01 UTC	435	IN	Data Raw: ae 79 0f 93 d3 00 c4 32 4b d9 3c 67 db fa 67 ae 74 ba 73 49 28 69 32 a7 4c e3 bc 5e 57 4c e2 76 75 7a 77 11 e1 fa d7 71 3c 1e bd 39 02 d7 3d b1 a2 44 39 ab c8 b3 04 32 79 f7 c7 1c c4 37 eb db 8e 1d e6 5c 49 eb b2 64 e8 10 92 d7 21 24 46 32 90 21 16 35 16 90 d2 49 c8 09 cd 5c ee 76 b9 93 fd 0f 1f 5c 5e 9b db c1 e8 5a a1 62 35 6d 2d 7c 5e 93 2f 37 16 24 07 3d 92 55 e6 5a b5 9d 3b 0b 52 d5 61 46 3c 94 d5 5e 72 fd 78 e9 3d ef e7 7f a2 7a f3 76 76 dc 64 98 4c ec 32 4a 13 24 24 98 74 92 24 ce a9 27 19 3a 3e 4c 9c 1f 37 d8 fa ae 76 d6 1d 77 2a 29 d9 d6 64 50 ad 5b 65 cd 92 67 6e 73 bb b2 d5 41 d1 2a 60 76 bc 4c 77 5b 39 9a 3d 21 20 35 61 13 32 bb 33 89 9e 23 fc df ed 1f 39 ca e4 99 31 a8 16 d4 f3 a1 4c cf 2c 9e 2d 2b 1e bc 0b de 9b e5 1e 91 d3 1d 35 0c 6c af 57 Data Ascii: y2K<ggtsl(i2L^WLvuzwq<9=D92y7ld!\$F2l5l\lb5m- `/7\$=UZ;RaF<^rx=zvwdL2L\$!\$!>:L7vw*)dP[egnsA^vLW[9=! 5a23#91L,-+5lW

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	437	IN	Data Raw: 79 5b 4d fd 8f 13 e2 0f 13 e2 7e d3 f1 10 f9 e4 37 fc 82 41 40 ba 0b c6 54 bc 63 10 27 96 9e 16 2e c9 f5 45 7d ac d3 01 13 93 7b 2a 92 3b 64 46 a9 a0 45 e4 2a 53 06 3b 38 34 3a ca ab b1 80 4b 75 5e 2b c5 a1 15 4a d7 b6 b3 f1 66 46 bf a6 63 fd 2e 0f e9 e4 74 fc 4b a5 fe 9c 6a ec b7 fa 86 33 51 91 8d 90 7b 23 9a d5 c8 5a 81 25 cf a2 cc 5a 25 33 8a 6e a4 dc d3 28 7a bc 7c 15 b5 55 b9 97 83 8c b0 e9 d5 f5 09 e4 dd d9 dc 31 9d 8c e4 85 53 5c 80 04 96 d8 f2 02 85 59 6a f2 01 a2 af 27 c6 e9 57 3c c6 c6 a3 19 7f 4d d5 5d 32 aa 7a 6d 1c 87 b7 17 53 0a 83 91 6a e8 01 3e 6c 3f 0b b9 b9 dc 02 2d 91 ae a9 5a bb d7 43 22 1b 15 98 2d 46 36 35 44 0c 3b ad 94 74 3c c7 94 74 1c 75 94 61 e1 d1 37 f7 dd 7d 34 cf aa e5 35 9d 64 6c 6d 59 f7 6e 5b 6d 75 2e 47 a8 3a 45 33 27 Data Ascii: y M~7A@Tc'.E [*;dFE*S;84:Ku^+JfFc.tKj3Q{#Z%Z%3n(z U1S Yj~W<M 2zmSj> ?-ZC"-F65D;t<tua7)45 dlmYn mu.G:E3'
2022-07-01 14:30:01 UTC	438	IN	Data Raw: 27 4a 3f d9 f5 9d 3d de 82 61 ff 00 0f d0 97 73 e9 7f 0f ed ea 24 fe d4 06 03 01 8a d1 6c 31 32 18 c4 cb 78 99 8d 17 30 cf aa 33 ea 8e 9f 20 80 f9 0d 1a d3 1d cc e7 e7 73 94 57 fc ba d5 f5 a7 4e 6a d8 c4 c5 66 5f a4 96 d0 82 58 aa 90 2c e7 a8 d9 6e b1 af 28 16 fb 0a fd 4d 9b c7 b9 9e ce d7 03 61 ba 55 62 4c ba eb b3 23 d3 d8 e2 8e 9f 32 0a b3 51 fb 74 14 7a a7 18 5d d5 ba 06 df a1 fd 23 2b 57 e1 3f 57 d6 d9 89 5f 4f c9 e7 aa ab 6d 54 b5 53 0d cb b1 7e 41 9c b2 d8 33 df bf ef 18 bc 84 2a bb 7b 90 32 bd 24 94 d4 c5 c3 b2 f3 87 d2 15 05 97 63 e2 82 d9 77 ca 71 eb a8 fd d5 7f 6b 2f f5 49 d4 b9 9b 7a 26 28 e3 ef e2 1d 19 ae db 83 ee 4e 81 ce c7 df 73 31 e7 d3 dc f2 ac 5c 7a 8b de 05 39 1e a6 ca b0 64 f5 0c dc 95 35 33 4e 98 5e 8b d7 84 a7 b9 6b 51 81 63 d7 4e Data Ascii: 'J'?=as\$!12x03 sWNjf_X,n(MaUbL#2Qtz)#+W?W_OmTS~A3*{2\$cwqk/lz&(Ns1z9d53N^kQcN
2022-07-01 14:30:01 UTC	439	IN	Data Raw: 80 d9 f1 87 f8 db ea 8a 3b fd 0b fc 4f 41 5d bc 67 8d e2 7c 5a 74 a7 a8 63 fd 3e 4f b6 d6 68 c5 5d ce de a0 d3 40 78 c0 77 2b 78 de 02 79 9f 31 46 a1 1e db 4d 3e 60 f9 c8 ab bb 8b c8 89 dd 0a aa c1 a2 6c c3 64 5b 6c 27 be f0 b0 2d 5e 47 9e e2 cf cf 8e f8 cc 87 36 1f 4b e3 f1 aa 37 3e 19 4c 93 1d 54 56 25 bf 1d 4b f1 cd c6 f9 fb 5f 1a b3 2e e9 fa 64 b0 82 b7 88 aa b1 d3 84 a5 74 27 a9 b2 7e 9f a5 67 36 b1 e9 a9 d5 55 3f 1e 0c b3 8f 75 31 7a 53 d8 b8 98 78 d8 a3 ed 3e 47 eb e4 ec 00 43 0f 76 75 52 c6 d2 2b d4 77 6a dd 32 15 a7 e2 d3 40 4b b5 6f 8b 8a 2b a1 6c 12 a0 e2 31 10 e8 c7 c6 42 5b 13 43 aa 7a 7d 72 f3 3a 56 16 2f 4a c7 6c ec 5a 21 ea 37 df 4f 1e a0 cc d8 58 8a cf 76 3d 97 f4 fc 9b 2e cb ab f1 cd 4e 9b 2b c4 c7 af d8 b0 13 67 66 78 33 cc c9 4e Data Ascii: ;OAJg Zic>Oh @xw+xy1F>'ld ['^G6K7>LTV%K__dt'-g6U?u1zSx>GCvuR+wj2@F?*1B[Cz]:V JlZl7OXv =.N+gxf3N
2022-07-01 14:30:01 UTC	441	IN	Data Raw: ca 7e 66 f4 54 ea 6f 73 73 e3 db 73 e0 0f 3e de a7 a8 2d cf da 95 da 82 16 ad ca 14 2c 6b 5d 82 ce 3b 97 ab 73 b9 85 f7 d8 d5 fa 5a 82 f9 5f 63 a2 38 7c 4d 4b 71 bb 76 a9 dc ea d6 5b 66 36 09 d3 89 f2 1a 95 9c af ae 30 c6 2c e7 22 b9 41 ae c9 6b 6a bf cc cd 0e 53 aa e5 7d 26 16 47 2a f0 7d 21 90 a7 17 f5 db c1 fb 42 42 42 ad 39 09 71 b1 bc d3 e6 0f 6f 8f 76 1b 8a 48 27 db 73 73 73 7b 99 4b b9 8a dc 4f c4 cd a0 32 ba 70 62 74 31 ef 60 f8 f7 0b 11 be 2f a6 5b 5e 8f b1 65 1e de 67 83 3e 21 20 cf 22 5d f8 66 1d ec 8d cd 09 c8 6f 66 7e 53 c1 03 db 0b f1 1f 69 8d 3f 65 c6 75 0a 7e 9b 3b fc 3f 49 5d da eb c4 72 5a db 95 7e de 0c 7d a5 9a dc fd b0 34 d4 de e6 b5 2b 3c a6 f8 8f dd 0b 4a da 6f 71 5f c0 3e ff 00 13 7b 3b 9d 4a 94 c8 c0 4a 68 e4 d4 55 1a 9c 7e 29 4d Data Ascii: ~fTosss>-.k ;sZ_c8 MKqv[f60,"AkjS]&G* !BBB9qovH'sss{KO2pbt1`/!(eg>!' fof-Si?eu-;? Jz~)+4+<Joc_>{ ; JjHu-)M
2022-07-01 14:30:01 UTC	442	IN	Data Raw: d5 31 b2 7d 5b 89 df bb 17 a3 f5 4c 96 e9 9e 8f 55 98 f8 f4 e3 55 a9 f1 1e 5d fb aa a9 ae 34 06 1f 9d c1 37 ed 61 96 72 22 df 33 bf a3 46 46 85 77 ee 07 1a 77 f1 7b c2 fc db fe 9b fc fe 78 d8 9b 8f 2d fc 4f f1 fa ce ca 8b 93 d7 3a 65 27 2f d5 0c 23 f5 bc fb c5 e9 7d 76 f4 4e a5 99 99 8e 2a 4e 2d 83 4d b3 ae e3 25 19 d1 65 28 ac cd 7f c6 ab 51 78 7a 7a df a6 eb ff 00 13 af d1 f4 fd 67 fc 3f 4f 5d d8 eb 72 9e 5a 8c aa c7 b5 5c ea 49 da ce d9 83 66 7e d8 0e e0 59 75 f4 d5 2c ea f8 a9 2e eb 59 0f 1e db ae 8a ba 9f 89 81 61 02 06 f3 ad c5 11 17 52 80 04 a4 f8 49 9d 8f f5 38 ce 74 dd d5 66 fc a7 f7 0c 3f 96 47 a7 b1 bb 18 19 cf aa fa 6d 56 94 af 38 d4 9b 12 d0 cc 95 77 4b fd 9d 43 43 aa e0 ba 25 34 ff 00 b7 65 35 d9 05 76 d6 85 a9 ef 85 b9 df ec f5 76 47 6b a7 Data Ascii: 1 [LUU]47ar*3FFww{X-O:e'##jvN*N-M9e {Qxzzg?O}rZl f-Yu..YaRl8tf?GmV8wkCC%4e5vvGk
2022-07-01 14:30:01 UTC	444	IN	Data Raw: 56 3b 73 a3 ef f5 a5 1c b0 87 d8 77 12 52 af 2a ac c0 80 c3 5a 4e 3a 81 09 5a 58 a3 0d 30 f1 12 2f b7 5a e9 f5 e7 63 8c bb 3a 75 d4 e6 f4 dc 95 cb e9 cd af 4f fd 3e 26 4e 2d 35 c6 ea 59 98 73 17 33 07 a8 27 69 d6 1b 59 62 d5 43 bd f8 98 b9 53 b1 9f 8f 06 78 ae 02 18 64 e2 d3 7c 38 76 d1 62 65 5c 27 2a 9d 9a b6 9b b1 3c 3d 93 f9 cf ca 6c 8c aa c5 aa 37 76 bf b8 67 6d f6 6a 70 5c 3e ae 56 d6 4a 46 0e 8d d1 f3 46 7f 4e 82 51 e9 ee 97 4e f8 05 03 cc 5f 08 16 72 84 c6 6d 4b ad 22 59 67 e5 f9 6f 64 cd 08 d6 0d 8b 8e eb 64 e4 87 7e c9 ec d1 c0 d6 43 ac 3a db 03 0f 83 e6 0d 40 7d 83 79 6d c5 1e 26 a2 e8 8f 3e da 9a d7 b7 88 bf b7 dd bc 86 00 d7 d6 f1 8d 9d 21 2a 04 53 da 33 b9 70 5e 4d 63 eb 52 9e 05 2f 01 67 f1 60 65 89 5d af 43 b0 d9 62 41 6e 45 d4 e9 80 53 4b Data Ascii: V;swR*ZN:ZXO/Zc:uO>&N-5Ys3'iYbCSxd 8vbel*q<=l7vgmjp>VJFFNQNO_rmK"Yygodd-C:@ ym>!*iS3p*M cR/g'e CbAnESK
2022-07-01 14:30:01 UTC	445	IN	Data Raw: 70 35 66 a3 ce ca 58 7e b3 33 10 e1 f5 ee 61 e9 e9 59 2c 29 ea f8 33 1f ad d7 12 ea 1e be 91 67 2a 55 95 a1 9e a8 bf b7 d3 c5 9b 3d d6 27 0c 06 c9 c7 c0 c4 a3 ee df d9 b8 04 23 c3 6b 93 71 42 f6 78 07 42 d0 03 66 c9 07 8b 7e 3b 4d 4e 46 58 db 8c de 5b 90 80 6e 77 02 96 66 11 d9 b5 bd 41 67 90 58 8e dc ed c3 ad b7 88 23 43 b3 3e 08 f6 f3 00 1e cb 1e 16 f3 99 99 5e 28 6c ec ab 2d f5 70 5b 9c 02 c7 d2 f8 99 38 9d 4f d1 17 f7 ba 42 fc 0f 8f 6d fb 65 d0 32 b1 6d e6 ae cd b8 8e c0 ae 43 d5 7f 48 ea b5 f5 0c 1f 50 e4 e0 6b 94 d9 9a 89 5b 3b 62 74 0e ab 91 30 fd 39 5d 55 db 83 d1 f7 5e 6e 06 24 ca f5 15 b3 27 af 6c e4 75 5b 6c 47 b6 db 27 4e 46 6c 75 a9 d4 1a ee 51 67 73 7e 97 b5 a9 eb ff 00 a1 6d b5 d4 b9 1e a0 e9 54 cb fd 57 c8 63 75 ee a3 9b 9d 90 d9 6f 06 33 Data Ascii: p5fX-3aY,)3g*U=-#kqBxBf-;MNFx nwfAgX#C>^(l-p[8OBme2mCHPkJ;bt09 U^n\$!u G'NFluQgs-mTWcuo3
2022-07-01 14:30:01 UTC	446	IN	Data Raw: 02 3d 26 7f 69 a1 a5 0c 6c 64 d7 6f 8a f6 f7 0d 55 eb 80 32 ba b9 2f fa cc 87 83 a0 e5 19 83 d0 a9 aa 2a 05 1f f6 fd b3 5e 17 ca d9 f8 87 fc a7 52 2e a3 1e e1 7d 26 78 8c 67 2d 83 ae 47 e1 9e 72 da d8 5a 78 d3 dc 01 2c 65 36 01 16 ab ac 96 f1 a4 8b 39 45 60 63 31 09 a6 da 02 23 10 27 2f 27 41 74 18 b8 3a b2 a8 46 fd 88 9a f1 e3 df e6 08 8e 35 c9 49 2b 0a 42 0f 2d 92 2d 71 5a e5 63 52 dd 23 d3 5f d1 6e cf ce b6 eb 2c a3 1e dc 82 f5 9c df 4a 27 4c bf 29 ba 6f 46 a6 a9 9b d4 3a 6e 01 ea 1e a0 cd ca 3c 8c 65 68 d0 09 c6 2a 08 a0 09 f5 b9 35 25 99 59 86 12 5b dc 0d c1 59 82 a8 94 6e 0a 04 ed 20 89 5a 18 b5 a2 c6 8e 54 c2 10 cb 3b 62 2d 44 4b 19 55 39 92 47 23 00 32 bd ef f3 db 09 6a c3 ef a8 12 76 8e 82 34 ed 9d 94 d4 f4 b8 ff 00 d0 f4 e1 ff 00 b9 fb f5 35 35 Data Ascii: =&ildoU2/*^R.)&xg-GrZx,e69E'c1#/'At:F5l+B--qZcR#_n,J'l)Of:n<eh*5%Y Yn ZT;b-DKU9G#2jv455
2022-07-01 14:30:01 UTC	448	IN	Data Raw: e0 8b 2c f2 f6 73 17 39 e4 39 f1 e4 03 d9 1d b9 4b 94 89 d0 f2 7e 9f 32 cb 04 36 fe 36 5d 05 a7 5d cd 93 67 82 c3 6c c7 4e 49 6f fa f9 9a 9a 9b da 23 13 3f 95 3e 60 9f 22 7f 1a 10 fc ef 40 f9 82 7c 1f e2 7f 1b dc df 37 cf a0 f4 ec 5c ce af 94 f3 d3 59 9f 47 d6 fa de 35 f8 dd 47 a4 ae ef e9 b8 81 30 29 c3 c7 c1 af 3b d4 b8 d4 cc ec fb f3 48 65 9f 8e f4 b3 f0 10 71 9b 58 1e 0b 37 03 a8 8a 39 1c a2 54 33 93 15 87 25 64 96 1a f9 69 62 c0 40 3f 84 fe 78 89 f9 21 0e 0c e5 3b 93 62 3d ad 2e 3b f6 57 30 58 60 66 9c 03 4e 20 c6 55 d3 15 53 f9 18 17 ca 8d 4e fa ac fa 92 61 b2 c6 80 be 97 88 35 bd 21 cf 6a 72 0e ac cc 48 26 31 e4 30 f3 2f e9 b7 9e bb d3 2f c6 19 3d 30 11 95 d2 b7 f5 3d 26 77 fa 4e cd dd 26 59 67 4b 32 ae ab 8d 8b 5f f5 ac 33 3f ac e0 4f eb 18 13 fa Data Ascii: ,s99K~266]]g Nlo#?>""@ 7 YG5G0);HeqX79T3%dib@?x!;b=-;W0X'fN USNa5ljrH&10//0=&wN&Ygk2_3?O

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	449	IN	Data Raw: d4 e0 5d 80 89 f9 27 71 35 90 7e 98 7f 50 c3 dd 37 77 31 2d eb 47 85 59 fd 47 32 cf 50 3f 46 19 b5 65 a7 51 f4 ad c1 15 30 f1 8b d3 d7 28 bf 35 ba 57 a5 99 a6 4e 4f 47 e8 f5 75 3f 53 66 e4 46 62 48 95 9f 2e a2 7f 30 7b 08 16 00 74 39 46 e5 15 8f 14 68 20 81 52 5b 53 ca 8b 56 6d 7e 50 03 c8 56 fa ad 6c e4 03 45 00 c0 a8 22 85 31 d1 a2 8e 47 b7 f9 9a 4f 01 49 58 ca 77 45 ae 61 57 2c fc b7 f9 30 6e 2b 19 90 2d 85 0f b0 0d 13 96 c5 70 20 d1 35 68 b0 00 be a1 bd fe 6c b5 e7 6d a3 b3 82 ae da d6 a0 17 46 37 80 a2 f8 e8 f0 7c 8f 25 b9 93 db 71 3e 9e f2 52 ab 88 ae 96 81 48 24 c6 e2 d7 e0 25 73 f0 d1 ae a2 5b 1d 58 db 43 99 d8 69 50 60 8c 26 f5 2a 7e 47 19 76 2c 5d 0c 6c 9e 2e b6 2b 4b 3e 2c 06 30 f6 c4 b1 ec b1 13 c6 4f c6 46 44 6c af 3d c3 05 c4 17 b4 91 63 Data Ascii:]'q5~P7w1-GYG2P?FeQ0(5WN0Gu?SfFbH.0{t9Fh R[SVm~PVIE"1GOIXwEaW,0n+-p 5hlmF7]%q> RH\$<%s[XCiP' &*~Gv,].+K>.,0OFDI=c
2022-07-01 14:30:01 UTC	450	IN	Data Raw: 37 63 74 da 31 fa 16 5f a8 71 71 2b ce ce cc cd 7e 53 c7 bf f3 c4 19 db 33 8f 9d 7b 7c 7b 02 27 89 c5 4c e2 04 e2 27 6c 4e d8 9d a3 3b 51 69 3b 2b e0 2e 8c 47 3c 7b a0 95 b2 6c 68 32 69 5c 18 36 4d 65 44 56 57 8b 4d 44 35 15 4d 11 34 90 22 c6 ab c9 41 be 35 40 16 68 c0 1b 6d cc 02 5e 72 b8 1e f5 db 6c 97 11 f2 09 82 e2 20 bc c6 b6 0b 48 27 29 a7 d6 3c 5c c7 30 66 3d 75 db 99 cc d7 9a 81 4d d4 98 f6 d4 14 dd 49 2b 04 af 35 75 f5 a2 36 5b 38 5b f8 47 c9 2d 06 55 40 2d ea 23 9a 9a 2d 75 ca eb 47 07 12 8d 76 13 42 93 18 64 28 ed 5a 63 d3 64 e0 37 65 75 47 a3 1b 6f 8d 4c fa 7a 14 04 a8 12 95 ee ce d8 64 fd a1 b4 dc a5 9e 4f b6 f5 2b b3 90 dc 27 44 c3 35 19 76 31 ec c4 e1 ff 00 ac 07 bf 8a a5 72 92 75 27 19 08 20 85 b5 19 8b 59 01 9b 95 b8 8c d0 d8 65 76 ca Data Ascii: 7ct1_qq+~S3{[{'L'IN;Qi;+.G<{lh2\l6MeDVWMD5M4"A5@hm^rl H")<IOf=uMI+5u6[8[G-U@-#uGvBd(Zcd 7euGolZdO+'D5v1ru' Yev
2022-07-01 14:30:01 UTC	451	IN	Data Raw: d6 d4 52 a8 6b a1 5f 82 cf 13 6e 5b b4 84 35 35 72 5a f4 8d 5a 91 ae 45 3c 43 59 73 9d 5f 06 9b 9b 81 a6 fd ab f9 4f 0b ca 16 95 eb 61 41 9a d9 70 15 4c dc 27 64 9f 24 1d 24 10 2c d6 cd 55 aa 21 55 31 85 4a d4 28 e5 7f 73 56 72 d1 05 63 45 7f 1f 89 96 3d 64 16 42 dc 11 a5 88 90 55 53 2b 55 a8 ca 27 19 c6 6a 79 9e 75 ed e2 7e 3b e6 ba d8 d7 89 a1 34 21 9b 9f 33 53 81 82 b6 9d b7 10 2b 18 04 50 26 96 71 81 1b 5a 71 08 30 ce 04 cf c8 c0 8f 12 b1 15 44 ae bf c7 81 13 17 16 fc ab 7a 4e 06 36 11 10 7d 83 c4 eb 5d 3f 4f 72 59 3e 03 6c 90 9e 6c e4 54 23 f1 61 38 b6 f7 70 8a f7 4e eb c3 63 19 c8 ac 1a e1 63 f9 49 bd c2 c7 5d d3 3b bb 87 cc 3b 80 bb 1a 7e 56 c7 89 c7 4c 8a 47 1b 60 fa 8e 2c 6e 9a e1 02 f8 e9 78 16 e5 e5 7f a5 e9 58 c5 1a eb f0 33 ac e8 79 58 b9 b8 Data Ascii: Rk_n[f55rZZE<CYs_OaApLd\$S;UUIU1J(svrcE=dBUS+U'jyu~;4!3S+P&qZq0DzN6]]?OrY@lIT#a8pNcc[!;~-V LG^,nxX3yX
2022-07-01 14:30:01 UTC	453	IN	Data Raw: 3e 9d 39 9a 2a 07 fd 20 50 f8 dd c2 e8 a9 63 a8 9c 89 1c 3c 5b e1 59 18 d9 da 33 b4 f0 a4 e0 f0 a3 4d 19 a6 8a 18 95 53 34 62 21 33 b7 35 b8 10 13 db 9d b8 56 04 33 b7 3b 71 ab 85 35 0a f8 e2 27 1f 1c 7c 71 9c 27 19 c6 6a 0d cd 9d 03 15 a1 6d c3 f7 fa 4f ab fd 42 30 2a 51 e5 4f cd 7d 87 89 d7 b0 a6 50 dc 7a 6c 33 b6 40 6a ce b8 0e 5f db 9f da 8a 2b db 7e e6 30 09 c7 c9 1b 9c 40 8c bb 9f 33 e6 00 27 f0 8b 0d 6b be d0 8d 58 e3 5d 30 53 c9 17 1d 84 14 f1 26 97 86 99 e9 9d 2f 5e ea 15 b5 8b d5 4d 6a fd 47 26 ae a3 7e 1f a7 77 7e 26 2d 18 95 c6 fe dc 26 72 84 c6 8f e6 34 68 66 a3 c3 35 08 30 88 c2 54 48 8e e0 4e 6c 61 0f c8 f3 0c c0 72 0e 01 07 c8 62 20 db 36 ed 10 02 c7 e0 f4 e6 55 6a 5b fb c2 e5 59 92 c2 c5 7a c7 2e d2 e9 40 53 90 c3 59 03 72 c4 fc 6c 59 41 Data Ascii: >9* Pc<[Y3MS4b!35V3;q5!q'jmOB0*QO)Pzl3@j_+~0@3'kX]0S&~w-&-&rh4f50THNlarb 6Uj[Yz.@ SYrlYA
2022-07-01 14:30:01 UTC	454	IN	Data Raw: 61 f9 f6 22 18 7c 4d c2 66 e6 e1 32 c8 df 38 56 f1 98 95 26 65 d9 5d 07 92 5d d3 72 b1 c5 2b 8f 65 7f da a8 56 e5 ec c1 73 a6 b7 f1 b6 e3 2e b7 6a c7 f2 56 88 d2 b2 3d bf 96 9c bc b1 04 3c 61 e0 8f 6b 1b 8b 17 13 92 43 c2 78 9e 20 d6 d1 3c d7 5b 41 5e 43 0e cb ac 4a 1b 90 a8 c1 d8 05 4e 33 4e 58 6a 4d 94 21 fa 83 be 99 cf 33 2d fa 23 98 fd 0b 20 83 d0 b2 d4 bf 45 ce 96 74 8e a7 1b a7 67 a9 6c 5c f4 66 fa 80 dd c5 07 95 44 9e 3b 64 53 1a ba e7 1a 63 a5 10 d6 90 d4 b3 80 9d b1 38 08 12 30 f6 dc 26 7a 49 78 7a 70 b0 03 b9 36 62 33 99 e6 68 cd 7e 9e c4 dc df e8 fa 4a be de 1e 5b ea 61 dc 4e 4d 43 8a 4e b9 d6 b1 fa 75 7d 4b 3e fc fb c4 c6 4f 20 6c 84 85 00 8d a8 a4 6e b2 43 7e 5c b8 bc 08 ab 19 04 fc 3d 88 59 dc aa 35 ca d0 5f b5 d9 8c 6c 30 2b 6f b6 67 00 ad Data Ascii: a"lMf28V&e]]r+eVs.jV=<akCx <[A^CJN3NXjM!3-# EtglfD;dSc80&zlxzp6b3h-JjaNMCNuJ]K>O lNc~!~Y5_l0+og
2022-07-01 14:30:01 UTC	455	IN	Data Raw: 00 e2 98 9e 32 a3 5a a1 85 86 03 6f 2f ef 99 c7 22 1a c9 17 0c 7a 46 5f 52 a9 9e eb 5e d2 47 9a 9f e9 ef 47 16 27 be e6 e6 e6 e7 99 e6 68 c0 d0 98 ea b1 80 f6 f4 ff 00 5b 38 0b fd 7b a4 6b aa 7a 9e a1 5d b6 3d 96 7b 0f 91 16 6a 11 c4 a9 d8 1f 21 b5 09 32 d1 b8 3c 11 14 f9 a9 80 11 f4 57 f8 b6 bf 20 f1 20 ee 6f c6 e6 35 37 64 d9 d3 3a 45 58 d0 0f b0 98 4c dc 30 fc ee 19 b9 b9 b8 d1 8e 89 68 5b c3 b4 63 fa 43 ec dc 73 e2 fe 30 0d c5 5d 7b 50 fa 8a e2 57 6c 04 c7 5d cb 92 71 f3 8e c6 30 96 af 9f 8f 65 8b e3 db 50 ea 18 d1 e3 43 ec 25 8f 1d a0 8a 60 2b 39 c2 62 b9 9e 0c e3 15 8c 56 30 79 5e 06 2f 89 e9 0f fe 37 f8 a6 1f 16 c7 6b 37 fd f3 15 6e 83 7a c9 ea 18 b4 4c 9e af 73 a9 25 d8 46 d4 d7 86 f8 f4 ee 41 7a 75 35 35 ed af bb 44 42 7c 18 d0 fd a3 de bf 21 3c Data Ascii: 2Zo/"zF_R^GG'h[8[kz]=f]j2<W o57d:EXL0h[cCs0][PW]q0ePC%"+9bV0y^/7k7nzLs%FAzu55DBj]<
2022-07-01 14:30:01 UTC	457	IN	Data Raw: 8e 33 8f bf 81 19 84 30 6c 2f 0e 50 2f 81 f1 e3 4f f3 b3 c7 cc fe 3a 16 5a 51 75 a8 0c f5 1f 48 ba d5 3d ca 6d e8 be a9 ba b3 8b 93 4e 4d 3e c7 64 ff 00 2c ab 38 f8 75 8b a9 f8 fb 72 80 ee 72 9b 83 5a af 52 b1 c8 28 d1 d9 10 b9 0e 79 11 4a b3 ce 85 d0 d3 18 97 d4 e5 b8 07 df a2 3d ad a4 3c b0 15 24 c3 39 18 61 86 6e 12 21 6f 25 a1 68 c4 47 68 cd 0b 4d cb 6c 24 32 fb b4 d4 e3 3a 77 4a cd cf 3d 37 d3 18 98 e1 00 0a cc a8 83 21 ed 1f 48 1c fb 75 db ba 9d 34 74 ba f1 3e 97 d4 74 ad 79 4c 37 3a 41 fe 9d d5 e6 66 bf ae f5 6c 4f ae c1 1d 27 1b 5b ae 9a ba af d3 ff 00 50 23 d8 19 5c 42 66 e7 88 d1 d6 0d eb 63 db 5e df 10 9f 06 1f 63 1a 37 cf a7 46 fa e4 f5 86 10 b7 19 97 c2 90 a4 9f 03 ba c5 29 3b 6a 67 61 67 d3 d7 ae ca 89 c5 d5 bc ee 63 e9 f2 1b f7 7d fd 67 19 Data Ascii: 30I/P/O:ZQuH=mNM>d,8urrZR(yJ=<\$9an!o%hGhMI\$2:wJ=7!Hu4t>tyL7:Af!O[P^Bfc^c7F);jgagc]g
2022-07-01 14:30:01 UTC	458	IN	Data Raw: aa 17 da eb 6b a5 2d ea 40 b3 d5 91 95 7f 4f c5 fa c4 54 45 2e aa e9 9d 8e 71 72 fd 87 b0 8b f0 e6 6e 6e 6f d9 61 9a 80 79 e3 08 84 46 11 a7 a5 aa 61 87 47 01 ef eb 4c 5e 17 17 87 7a 55 dc e1 13 f1 8d f2 57 c3 55 ca 70 71 07 2e 3e 8f 1f fb 9f bf d4 75 37 d3 aa ee 04 59 f3 36 63 0f 0d c7 8e f5 15 8e b7 e7 cc 0d b5 f3 4b 4f 0f 99 60 11 a5 cd fd be 94 cd fd 4f f8 fb c4 e9 7f 97 40 d4 f3 39 00 49 10 fc 6c 4e 9d 7f d4 e2 42 23 a6 e5 d4 a9 8c 87 4b 4b 68 8f 3d ae a4 b1 5d 21 3f 8a 93 ae 40 8b 36 25 5e 40 5f ca e4 e0 3a 77 49 bf a9 bf 4a e9 f8 dd 36 98 b0 c0 77 00 fe fe 7e dd fb 84 42 21 68 5c ce 25 85 9b a6 0b 8f 2e a9 89 dc 47 3c 63 34 63 09 9d 1f a1 59 91 2f 44 a3 a7 54 48 15 93 bd 03 34 21 9b 30 99 a8 74 23 11 08 84 4d f1 6e 81 98 b9 58 ec 15 d4 d7 91 7a Data Ascii: k-@OTE.qrnnoayFaGL^uZWUpq.>uY7Y6c'O@9IINB~KKh=]!?'@6%^@_!jJ6w~B!h!%G<c4cY/DTH4!0t#MnXz
2022-07-01 14:30:01 UTC	459	IN	Data Raw: e9 1d 60 13 d3 7a b0 8f 81 d4 16 1a 2f 59 fb 67 71 67 a3 70 fe 9f a4 ea 6b dc 80 45 d8 e5 91 6e ba b7 47 ae d9 8f 4d 38 f5 96 3e df 91 9a 50 5a 02 cc bd b1 09 02 77 0b 8e 28 93 d4 98 0e e8 75 04 53 a9 85 80 db 4a f4 ab a0 17 e3 dc 7d e6 19 56 83 fb 93 3a c6 37 d6 74 ce 68 d0 3d 5a 43 5c 1d b0 ec 82 05 59 c3 c1 dc f4 92 eb a5 fd 99 99 55 e2 d4 3d ae be 8a a7 5c a8 3d 28 db 0a 27 c2 16 25 06 e7 c4 04 45 f3 ec cb 01 d4 e5 b3 f1 1f 51 99 b8 5a a3 58 7f f1 ff 00 47 1f ff 00 92 87 cf f3 b2 20 e3 18 9d 46 3f 96 f9 1e 8b 79 c8 e9 fe dd af 1a 00 6e 7e 51 ab 33 a7 f4 fb f3 ae e8 fd 2f 13 a6 54 bc 9a 2a 28 85 a3 3c 36 19 f9 19 c2 76 c4 fa 7a cc fa 4a 89 3e 00 68 cb b8 76 a1 1c 18 5a 6f 71 81 04 59 03 0f 67 59 bd 46 31 9a 16 85 e1 30 fb 74 ec 4d 9f b7 a8 ff 00 f3 eb Data Ascii: `z/YggqpkEnGM8>Pzw(uSJY:7th=ZC\lYU=!\=("%EQZXGF?yn~Q3/T*(<6vzJ>hvZozqYgYf10tM

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	473	IN	Data Raw: fe d5 2c ab d1 b8 65 c0 f6 a0 d8 06 05 e3 8a ce 3b 75 ed cb 47 b5 b9 63 9d 9e 57 52 0c 8e 5e 82 be 93 eb 35 bb 3f 68 e4 b0 7a d5 8e 1e 71 bd 03 53 c1 60 a7 68 cc a8 a7 3d bb d4 b9 be 37 52 e2 de f5 96 a9 6e ca 38 f1 48 e7 62 83 83 1d 41 be d3 ff 00 44 1c 5b d2 bf da 7f e4 17 46 d9 ab 57 d8 65 cf 7f 05 e7 6a 7a 2d f6 29 1b f7 bb f4 58 69 30 34 7c 7d 23 e8 fa af f3 8c ff 00 d4 3f 3f 49 23 3d 56 50 57 25 cd 43 8c 29 9d 79 d9 6d e8 75 1b 40 98 e9 31 5f c1 68 1a 4d 2a ee f9 b3 9d b6 d6 e4 ec bf 2f 2b 47 a9 f5 8d 33 f7 87 ea 02 75 5a 76 63 e9 b4 cc 6f c9 06 1d 28 17 c8 1b 7d 34 ee 7d cb 11 d1 ea 1f f1 eb 47 b8 2a 2c d9 0d a7 1b 21 b6 31 96 77 57 f7 a9 59 ea 73 39 4a 75 1f e9 bc b3 bb 31 ee 2a cc 03 b5 41 7f 70 5d 52 79 95 72 d0 a7 69 e7 25 ea d3 0a 1e 5f 52 d9 04 1c Data Ascii: ,e;uGcWR^5?hzqS`h=7Rn8HbAD[FWejt-)Xi04[]##?!#=-VPW%C)ymu@_1_hm*/+G3uZvco({4)G*,!1wWYs9Ju1*Ap]Ryri%_R
2022-07-01 14:30:01 UTC	474	IN	Data Raw: 73 8e 11 9e 43 50 73 5c 1a e2 ec 51 c4 70 41 b5 98 43 62 71 0d c5 0c 2e c4 0d c1 d5 87 06 20 eb 15 a3 77 84 7c a2 5b 2c 3f 57 f4 45 ec 6c 3b da a5 63 e0 a1 ae ee 5b 6d 53 45 e5 be f1 e0 ba 42 c2 c7 6f 7d 2f d1 5e 27 33 02 2f a9 e1 a6 1f 57 cd b7 bf 3f 72 a1 a2 b4 f5 b6 c8 1e e5 84 36 01 e6 80 83 cd a0 29 38 69 8e 32 83 7a 47 d4 71 dd 4c 5c a0 6b 62 a2 df 66 65 df a2 f3 14 9a d3 bc ef fe 58 56 68 97 52 38 bb 46 f1 e0 83 9a 64 11 23 c8 8c cf 01 9a fe 07 2c d1 8f 14 10 c5 62 b3 9f 22 08 56 d5 72 a0 94 46 6d 56 b2 19 bb 9a 3a 56 8f a4 bf 46 a8 ee bc 09 95 d0 32 a0 c4 e7 6d 39 d9 b8 a6 53 a1 4a 4d 5d a6 06 8c 21 c6 7e 32 83 e9 9a 74 85 5a 64 b0 0b d4 6c 1b 9f 8a 7b ce 39 05 af c5 50 c3 04 1f ff 00 eb dc b4 a7 54 d3 1a 1a f0 fc 4d 65 cb 5a ec 31 e0 50 c3 a3 d5 Data Ascii: sCPs\QpACbq. w[.,?WEI;c[mSEBoj/^3/W?r6)8i2zGqLkbfXVhR8Fd#,b"vRfMv:VF2m9SJM]-!2Zd{9P TMeZ1P
2022-07-01 14:30:01 UTC	478	IN	Data Raw: 39 ac d4 4a e2 84 c2 95 2b 3d 51 25 12 1c ae de c4 06 1f d9 39 ce 06 3e 2a 20 c1 52 37 2e b6 7b 6d 7d a3 56 52 b7 05 bc ef f2 fa 48 da 8c 33 cb d0 da 5d d8 8b 74 6d 0d 8d 1d 21 63 5f 51 d2 0c 6f 4f a8 ed 22 d4 cc 1a 40 61 ee 20 5d 0a ad 25 c1 de df 59 a7 78 2b 3d 57 6a 72 95 a4 e8 fe dd 3c 5e 0a ad 03 95 46 16 f8 85 7c ff 00 94 af 47 fa 9a a7 bd a7 f7 47 c5 75 dd ab 69 c0 76 94 f6 62 69 0e 11 d6 e2 a0 98 23 8b 57 c5 77 35 7f 7a ef 72 ea c1 bd a5 75 9c 7b 14 e1 6b 79 92 ba ce 77 d9 0a 70 b5 bc dc 54 02 e7 f6 58 29 76 0a 63 7f 15 77 9a a5 16 e8 d4 9b 4c 73 5e 72 a9 70 e0 16 5a a0 ea 90 b2 42 d0 11 0f bb 48 82 8b 0b a0 7a af e2 16 07 99 56 6b 23 9b 95 9a c1 1d aa d8 4f 60 51 26 5e 70 f7 6f 4d 3b 78 68 ed 19 cb 92 92 60 04 1c 40 3c 1c 83 43 c3 d9 bc 3d 61 6e Data Ascii: 9J+=Q%9>* R7.{}VRH3]tm!c_QoO"@a]%Yx+=Wjr<^FIGuivbi#Ww5z1rU[kywpTX)vcwLs^rpZbZVhK#O`Q& ^poM;xh`@<C=an
2022-07-01 14:30:01 UTC	482	IN	Data Raw: e6 a9 35 bc f7 f9 59 42 cf 55 90 b6 ae d5 c2 11 20 f6 4a da df bd 49 75 f2 ba 1b 57 df 28 e1 6a b6 c9 3b 97 1f 82 98 07 e0 a0 8e ad c1 52 1d 13 c5 0f 8e f2 b1 9c fd e8 61 74 1f 7a 89 46 d8 66 d6 cd 41 7e 4b ad 9e 5a af 08 ec f2 59 65 92 df 75 9a 9b 28 53 2b 35 92 bc 28 b2 cf 35 99 e0 b7 ac 34 d8 e2 5c 9d a3 54 a6 fd 26 b0 1b 4c 9c 2c ef 39 94 34 7c 6d a7 47 75 1a 7b 0c 0a be 88 5d 2e a2 ec 6c ec 3f ba a3 a4 0f ef 18 1d e5 8f 94 69 cd f6 6a f6 ee 2b fe 42 b1 76 1f 67 35 d5 11 e0 86 87 a4 3b f8 8a 63 64 fb 6d fd 55 4d 1c fa e2 c7 81 dc b4 2f 94 88 8a 8e 69 a1 5b 93 db ff 00 0e a2 1a ea 96 dd 9f 6a da 8e f0 86 31 2f 6d b1 71 1c f5 e2 a1 a3 d4 7b 7d a8 d9 f1 43 e7 1a 76 8b 4b 90 77 48 ef f4 af e1 f4 3f 94 34 ce 78 45 16 7e 6a da 3f c9 fa 08 e2 47 4a ff 00 7a Data Ascii: 5YBU JluW[j;RatzFfA-KZYeu(S+5(54t!L,94[mGu[.! ?ij+BgV5;cdmUM/[j1/mq[?CvKwH?4xE-j?GJz
2022-07-01 14:30:01 UTC	483	IN	Data Raw: dc 6d c2 ef 10 86 2a 87 44 ab c1 ff 00 aa a2 34 7a fe 72 a3 e4 39 be c8 4d a9 a4 06 12 c6 e0 11 64 07 ad ec ac 6e 38 79 2f 36 6f 9a 65 4f 68 03 e5 5d 59 5f 56 57 46 2e bb 3c 10 22 49 17 c8 9a a0 18 58 70 a9 9c 32 84 3a 78 a3 2d ec 85 85 8e 89 e0 80 39 72 fd 57 52 4a 12 e9 c3 e0 ac e9 08 4c 5f 34 49 ca 6f 25 c0 ac 30 21 4b 81 69 2b 09 7e 48 d2 10 ae 33 cd 7d 95 d7 89 c9 6c b8 42 1c 37 ae a8 44 e0 b8 c9 44 2d e2 54 4e 4a 41 0b 2e d5 8a 14 5d 4c 15 61 92 dc 1b 9a a3 a1 57 65 ab 34 ed 62 df b9 55 a2 f9 2f a6 e2 0a 6b 69 68 ee ae 77 b4 09 54 fe 4e f9 4d e6 a5 66 54 2f 6b 28 38 12 ce 44 e5 c5 61 d0 28 33 42 67 b4 db d4 3f 7b f4 5d 21 71 2f 99 c4 73 55 f4 77 1f a5 a7 23 b5 bf fb fa 0d 29 91 b2 f7 74 8d ef 5c 17 15 6b 2c d4 50 d1 ab 55 fb 2c 2b ce 52 a7 40 71 a8 Data Ascii: m"D4zr9Mdn8y/6oeOhjY_VWF.<"IXp2:x-9rWRJL_4lo%0!Ki+-H3]JB7DD-TNJA[LaWe4bU/kihwTNmTf/k(8D a(3Bg?[]q/sUw#)tk,PU,+R@q
2022-07-01 14:30:01 UTC	487	IN	Data Raw: 2b 7e ab 37 c1 75 5d e0 a0 b4 85 bc f7 6a 8b d8 ab 35 75 55 95 f5 6e ef 50 44 ca b4 80 ac ae ac 54 b5 4a dc 15 88 f1 59 eb b9 5d 65 65 8b 25 72 4e bd 90 2d ab 3d 5c 15 c9 57 5b 45 1e 3c 56 1c 06 50 1d 13 a5 02 da 0e 2b 66 82 00 2a 1e e6 0e d5 9c 2e b2 cd 66 b3 59 ac ca b1 95 97 93 4a a4 f5 5e 0f bd 0a 95 b4 ca 8f ab c7 46 64 88 ef 55 34 6d 16 be 95 38 76 69 b9 9b e7 79 53 c0 79 13 b9 59 71 0b 64 c1 57 5b 2e 01 71 57 30 ad 25 6d 01 d8 ae 16 3c b8 ab 0c d6 6a 2d 2a e6 fc 14 85 9f b9 5c 95 6c 94 64 ac 9a cd ee cf b1 43 37 21 28 dd 4a e9 41 b1 dc a2 65 08 c9 6e ef 52 26 02 c3 bd 48 16 50 49 50 43 88 44 90 3c 55 81 85 94 77 2b 23 88 ac ee 17 56 f9 5d 6c 5f 9a e2 77 05 76 dd 1d c8 d2 39 3a e1 6 2 10 b8 a9 1b 95 fd cb b1 03 d5 50 32 5b c4 f1 59 59 67 9e 4b 21 Data Ascii: +-7u]5uUnPDTJY]ee%rN-=W[<VP+*.fYJ^FdU4m8viySYqdw[.qW0%m<*-]ldC7{JAenR&HPiPCD<Uw+# V]l_vw9:bP2[YyGk!
2022-07-01 14:30:01 UTC	492	IN	Data Raw: 77 48 e6 b6 aa 09 ed 44 16 ca b8 d5 00 df b5 5c ac f5 65 ab 24 56 67 5c 59 70 f2 33 3e 0b 32 a2 ea c5 66 b9 2d ca c8 2c d7 aa b7 2b 7f b9 44 ba 54 62 1d 85 5c 6a cf 54 97 2c dd 2a c4 a9 91 1b d6 10 47 14 04 b0 f6 2c 2d 17 71 80 17 4b a6 b1 85 fb a9 e6 07 92 6b 52 eb 01 b4 38 85 88 65 da b6 59 8b bd 43 a8 d3 56 a7 85 75 1b e2 be 88 2f a1 9e c5 87 a1 8f 05 7a 6e 1f 75 76 72 56 76 2e f5 72 40 56 aa ad 50 78 28 c4 3c 14 e3 57 a8 17 d2 7b 97 d2 85 b5 55 5a 0a 1e 76 3b ec b6 9d 7e d5 b3 56 0f da 5f 4f 8b bd 47 4c 1a 3b 25 48 d2 5a 7e e0 58 9d 54 3b ce ee 80 b6 6a ab 55 3d e1 7d 2d fb 17 5c 78 20 7a 51 e0 55 ea 01 dc ba 2a 0e e9 5f c2 17 ce 74 b7 b5 f5 00 99 39 37 b1 6c 39 a0 3b ab 03 12 c1 50 6c b2 70 ef 27 b5 cb 47 d2 1a 1a ec 2e 2c 31 c0 ee f1 0b 47 d2 1f 06 b7 Data Ascii: wHD\e\$VglYp3>2f,-,DTb]T,*G,-qKkR8eYCVu/znuvrVr.r/VPx(<W[UZv;-V_OGL;%HZ->XT;ju=->-x zQU*_ t97I9;Plp`G,.1G
2022-07-01 14:30:01 UTC	496	IN	Data Raw: 0a b3 b4 91 ff 00 91 5b 4a d2 47 e1 2b 67 4f a8 3b 69 05 b3 a7 b3 be 91 fd 56 c6 93 a3 1e dc 41 5b e6 ee ec aa bf b2 87 76 56 6a be 81 5b ba 0f e6 af f2 7e 97 fe 51 55 2a 69 6f d2 28 38 54 c3 87 0c 6e e6 ae fd 29 fd b5 07 e8 bf b1 e2 fb 4f 25 36 95 36 06 b1 82 1a 38 7f 26 43 4c 15 67 80 2f fb 2b d8 79 6d a6 c1 2e 71 80 a9 e8 ac f5 05 fb 75 3b 49 70 f3 74 b2 e6 e5 26 c1 1d 1f 47 da ad f0 ed fd 13 aa 55 79 73 dd 99 d5 60 af 74 38 2e 0a 1b 2a 4d 5f 5f 24 23 ab c9 5e 3b 65 10 f0 7b 57 d1 82 dd c5 62 28 f5 8f 7a 16 e6 a7 0a 8f 81 53 31 c9 45 bb 95 85 8e 7e 5f 44 62 38 af dd 75 a3 b1 1d a9 30 b0 b1 bb 3e b3 8e 41 74 74 59 03 79 de 7f f9 05 3e d5 73 64 d7 bd bd 5e aa 10 2d e4 46 ac b5 e5 ab 77 a1 b4 77 ad b1 0e d7 96 bb 07 78 2c de 16 7e 2b ad 84 2e bc a3 35 50 Data Ascii: [JG+gO;iVA[VV][~QU*io(8Tn)O%668&CLg/+ym.qm; pt&GUys`t8.*M_\$#*;e{Wb(zS1Ev_Db8u0>AttYy>sd^ Fwwx,~+.5P
2022-07-01 14:30:01 UTC	500	IN	Data Raw: b3 86 c3 b2 42 9e 89 43 18 f6 b2 68 58 74 ca bd 2e 3b 1a 63 20 9a 45 3e 8e 7d 5f 23 a3 a5 3a 4d 6f 62 95 fd ea 2b d5 f9 9d 33 fd d5 3e b9 53 4e 98 63 bd a3 b4 ff 00 1d ca c3 bf 7e ac 75 5e 18 d9 8b a6 33 45 66 3a 8e 2e 6e 17 ec ed 0f 57 91 4e d1 eb 63 c2 f7 bd 95 07 aa 69 91 2c 78 dd 63 65 56 a6 99 f4 87 0d 3a ad 16 da a6 7a d2 9c 5a c6 b4 bb 38 19 a2 c7 5d ae 10 55 5d 1d d7 e8 dd 1d be 83 8e b9 91 e4 fe fe 4d 6a c6 a1 a3 4d cf ab 7b 50 bf 85 a4 6a 10 60 bd da e9 e9 cc 16 7f 9b 7f 6e e2 a0 a9 68 57 53 96 ad e1 71 ed 5b bb 96 e2 a3 02 f1 56 8b cf c3 d0 74 ec 7b 84 40 74 70 53 9a 05 c1 18 b2 3c 75 5b 3e 28 09 24 fe 48 8f 05 04 d9 4e 4a 66 e8 d9 75 88 dc a6 75 49 de 8b 91 24 df 09 f8 1f 45 a2 72 a9 50 7c 11 85 21 5d 4c 67 aa 2c a9 d5 3d 68 87 f6 f9 04 10 87 Data Ascii: BChXt;:c E>}_#;Mob+3>SNc-u^3Ef:.nWNci,xceV:zZ8]U]MjM[Pj`nhWSq[Vt{ @tpS<u>{(\$HNJfuul{ErP!]Lg,:=h

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	504	IN	Data Raw: a3 b4 1e 96 e1 13 48 0c 3b a1 38 de d4 89 30 83 cb 61 a4 4e 69 bd 8b ef 3b f2 f4 53 ea 6d 9e e5 2c 01 82 d7 41 b7 a8 e9 f0 47 a5 76 11 c0 28 a0 c8 1e d1 4e c6 e7 69 0f e1 c1 43 c0 a4 cd c1 a6 e1 3e 97 b2 63 cb e3 e5 5a fd 8b aa 1b da 55 df dc 04 2c a7 b5 75 1b e0 bd 5f 05 2e 6b 7f 08 58 45 36 04 cd 2f 0e c3 f6 5c 79 a9 b0 fb ab ac ef c0 ba ce fc 2a cd f1 44 f4 6f 5f 43 75 b5 84 77 ab 38 47 62 d1 a7 11 82 4e 5c 8f a1 10 d1 6c ad e4 b7 49 68 eb 58 f6 ae 0b 82 df 27 9a 9c 26 c8 91 12 a4 e6 ae 54 64 a7 0c 2c c1 ef 5b cc a2 66 0a d3 3b 5b fe ef 45 23 d7 9d d1 a9 fc 15 e1 c8 d4 55 f5 7c 35 f0 3e 96 14 ea b6 a8 3e 54 05 65 d1 bf 5f 4f 50 45 b6 47 f2 07 b0 a1 a9 df e2 bb f2 4d 61 de a1 16 89 4d 71 39 89 c9 58 8b a3 b5 11 c5 12 2a 0b 2e b0 58 a3 64 a1 21 1a 9a 3f Data Ascii: H;80aNi;Sm,AGv(NiC>cZU,u_kXE6\y*Do_Cuw8GbN\lhX'&Td,[f;[E7HUJ5>>Te_OPEGMaMq9X*.Xdl?
2022-07-01 14:30:01 UTC	508	IN	Data Raw: 7e a7 22 2e 0b 6f d3 24 c8 69 c9 4e 26 d5 ad 83 6f 8e d2 90 1e 0f ba 58 a9 5f 16 7f a8 e3 dd 49 0f 2c be 97 81 28 36 b1 2e 96 cb eb 3a d5 9f bc b4 0e 9e f2 f3 39 a4 f8 2c bc 20 68 ab 7f b8 85 ca 31 9b db a3 d6 56 24 d3 ae ff 00 5e 9f f9 32 2d 67 6d f3 e8 fd e5 a7 c5 74 e6 06 ed 96 2b 35 0d d1 72 04 cc b3 d0 1f a8 45 57 7c 34 fb 30 aa b3 1b ba 25 46 be db 8f f3 50 2f f5 33 1c 3a 33 8f b6 a0 5b 36 cb 8a 3d 35 d2 67 8f 03 5e 60 b9 9e ff 00 88 8e c6 06 dc 3e e4 56 61 57 2a f6 c4 a5 7c a0 2f c9 0b 68 97 43 1e e4 4e 61 99 bb cf ad cc b4 56 a9 4f de 07 59 74 28 fa ac dd 6a 75 6f cc 03 da d7 cf 33 36 2f a4 cb e1 84 37 a6 ec 60 f5 63 e6 50 bd fa 68 f4 42 75 74 c3 7b 04 a7 ab 9a 45 f5 dc be d1 95 2a 57 d0 8d 83 88 0a 5e 17 72 ed 1e 5b 84 5b 9e 3f 48 1b 90 f5 72 fc Data Ascii: ~".o\$!N&oX_!,(6:~9, h1V\$^2-gmt+5rEW[40%FP/3:3[6=5g^>~>VawW*/hCNaVOYt(juo36/7`cPhBut[E*W*r[[?Hr
2022-07-01 14:30:01 UTC	512	IN	Data Raw: 5f f9 cc f9 fe c4 c1 8d cf f6 8e 0f 42 00 90 1a 02 89 72 fe 99 7e a7 7c a7 e3 96 26 27 aa a1 c5 e7 a5 71 08 1b 28 09 b1 2e 96 cb eb 3a d5 9f bc b4 0e 9e f2 f3 39 a4 f8 2c bc 20 68 ab 7f b8 85 ca 31 9b db a3 d6 56 24 d3 ae ff 00 5e 9f f9 32 2d 67 6d f3 e8 fd e5 a7 c5 74 e6 06 ed 96 2b 35 0d d1 72 04 cc b3 d0 1f a8 45 57 7c 34 fb 30 aa b3 1b ba 25 46 be db 8f f3 50 2f f5 33 1c 3a 33 8f b6 a0 5b 36 cb 8a 3d 35 d2 67 8f 03 5e 60 b9 9e ff 00 88 8e c6 06 dc 3e e4 56 61 57 2a f6 c4 a5 7c a0 2f c9 0b 68 97 43 1e e4 4e 61 99 bb cf ad cc b4 56 a9 4f de 07 59 74 28 fa ac dd 6a 75 6f cc 03 da d7 cf 33 36 2f a4 cb e1 84 37 a6 ec 60 f5 63 e6 50 bd fa 68 f4 42 75 74 c3 7b 04 a7 ab 9a 45 f5 dc be d1 95 2a 57 d0 8d 83 88 0a 5e 17 72 ed 1e 5b 84 5b 9e 3f 48 1b 90 f5 72 fc Data Ascii: _Br- &'qxcvnil8a OK&3{!L0LW'AdY(i)L r^-s(h?~+cBLF%8Uar*5){t=Q"?~iMi!~miM4">rsldnYzBeq1
2022-07-01 14:30:01 UTC	515	IN	Data Raw: a5 15 83 e2 64 0b ae 9c 67 73 84 8a fe 23 c5 80 62 dc 7b 5a 42 57 2d cb 4d 7d 8b 8c af 09 69 28 72 e1 d3 5f 79 78 39 ac 22 b8 ad 7a be 9f 44 0a b6 8d ad 5c bf 6f 69 e1 8d 16 3a cf 79 79 99 78 9b bf 0c cc 93 e8 44 45 12 93 c5 f1 02 f7 14 6d e6 70 78 1b 7a 37 16 f7 53 5e 8e 1b 59 9e b2 53 39 3d 22 5a 98 da 3a 72 fb c2 b0 1b 74 93 35 f8 99 fa 19 4f 4c 7d 16 bb 46 f4 21 bb 35 f4 6b 6b c6 21 71 f8 cb e1 de fe c3 1e d1 b0 6e 9f 77 a0 94 89 5b df ef fa fb ce c8 e0 ef cf 2f af d2 e5 fd 2f fc 87 97 8f fd 77 15 da a0 5c 55 d4 fd ce aa f4 84 f7 0a a7 a6 25 4e a7 41 44 57 63 f2 40 f5 de ac d4 3e 3c 43 7c 5e 67 4f 68 8b a1 f7 4b 96 54 96 ab e6 0a 2c 38 6b 15 3a 70 3e f0 4a 26 77 99 51 5d 39 9c e1 5e 0e 26 2b 54 b1 95 73 2c 51 bc be 23 77 0f 0f d9 1e 0a 1b e1 ac 4a Data Ascii: dgs#b{ZBW-M}i(r_!x9"zDloi:yyxDEmpxz7S^YS9=={"Z:rt50L}F!5kk!qwn[/!wU%NADWc@><C[g^oHKt,8k: p>J&wQJ9^&Ts,Q#wJ
2022-07-01 14:30:01 UTC	519	IN	Data Raw: 78 4b b0 5b e7 e2 0d d4 07 e9 15 bd 60 d1 ed 39 67 72 a5 c5 cd f1 44 4c 0d 2f ce 7c 96 5c b5 34 44 31 11 d0 e2 41 c0 aa 6b 77 30 5c 6d 92 fd ed f1 2f cb cf 9b 7f 32 a6 03 b9 cf a4 a3 bc d6 4d 2a ac df 5a 08 04 c2 52 50 ce de 90 df 29 55 cd af 96 7d 23 31 02 d5 70 43 aa 1c 96 cf 0c de 93 43 b6 b1 a6 06 90 15 4e 23 49 a4 43 5d 31 eb 70 8e d2 00 9e ff 00 e0 cf 06 5f 28 a8 fa 87 cc c9 93 a9 09 ff 00 b5 3d b1 a1 28 68 48 83 2b d1 8f 73 fd 47 be d5 23 2a 3a 23 99 0a da 08 57 93 ec c1 06 5b 1f 07 d1 4c d2 b0 94 df e6 54 50 ec 17 c1 7f 69 70 63 1e 97 b4 fb 21 44 b0 43 82 a1 53 01 6b 77 30 df aa bb 3f 30 76 03 73 da c0 25 b8 f4 3f 98 e1 a7 7f e1 50 ff 00 11 b7 8e 4b f4 35 eb 52 dd 40 43 b8 bd 7a 33 13 8d d0 55 ea ef e7 da 51 91 25 48 30 d0 e8 e4 e9 29 ed 0a d6 ae Data Ascii: xK['9grDL/\!4D1Akwo!m/2M*ZRP)U)#1pCCN#[C]1p_=(hH+sG*#:~#W[LTPipc!D3Skw0?0vs%?P K5R@Cz3UQ%#H0)
2022-07-01 14:30:01 UTC	524	IN	Data Raw: 0b 36 43 66 0e 55 70 f8 58 50 71 d2 fd e7 8b 65 a7 7c 6b b4 33 07 78 c6 d1 b6 98 6d 2f 58 a8 5b 94 ed 96 36 46 df 41 3c 30 91 98 3d 99 80 66 6f 7c ed f3 2b d3 72 ef 71 f1 fe 4a 80 c1 81 95 e0 cb ed 32 3c 73 e5 14 94 49 fd 2f ed 61 f3 28 d7 7a 1f c8 63 22 53 85 50 00 2f 80 3d 8f a2 bf c9 19 40 2b 8b 6a 31 4b 92 5d eb 7d 82 5f d2 ea 7b 29 fe fb 4b 4d 22 d6 95 d5 8b 7a e7 da 08 c4 0f 06 ec 35 e7 24 c5 3a a5 27 de 3d 2c 5e 90 54 38 e5 6a b3 08 5d 1e 8b 57 68 7c c4 b3 64 78 e1 66 60 14 ce 7d a6 eb 91 c4 22 1b 57 7a 9c 08 4b ea b0 ea 78 c6 d4 87 b9 2b e6 0b 8d 98 c2 cd 13 87 8f 12 dd c7 7c 89 84 48 60 eb 0e aa ba e7 30 7c 4a 1b a4 dd f2 4b 45 97 62 17 d0 8c 46 85 dc 67 55 4b 48 ee 5e 0e e2 0f 36 77 c7 a4 2c 1a 44 ad 5d 0b 0a 89 84 d2 31 31 a9 e5 f0 5f 9b Data Ascii: 6CfUpXPqe k3xm/X[6FA<0=fo!+rqJ2<sl/a(zc"SP/=@+j!KJ)}_!KM"z5\$:'=,^T8j]Wh dxf}')WzKK+ H^O JKEbFgUKH^6w,D]j11_
2022-07-01 14:30:01 UTC	528	IN	Data Raw: 86 ad 57 81 88 5e bf e5 51 5d 41 32 a5 f4 35 7f f7 c4 f1 a8 2a 54 a9 52 be 95 2a 57 d6 8e 10 e0 6b a0 29 d1 32 65 66 40 16 31 9c 86 19 42 22 27 05 a1 c1 ca cd aa 61 c0 6c a0 72 5b 49 9c cb fb ef 0a 96 57 20 72 cb 35 da 59 0c a2 34 84 42 0e ad 18 36 5c 4b d4 17 de 42 32 3b 63 12 88 19 8e d0 59 a7 a0 99 2a 17 02 63 da 12 e5 37 ad 4a c0 d0 26 65 59 6d 31 fe a3 ca 97 ab b3 ef 35 22 c0 e7 3e b1 d2 c4 a8 e3 97 bc ce 67 7b a3 ae e6 55 6c a5 53 93 de 1d 35 8e 8c b3 5b de f2 c2 da 00 b7 6d cc 4e 27 a0 96 39 58 9e 99 a4 cd f9 23 ca 38 0c a8 ba ce fc cc 45 4f 58 05 65 10 2c 04 c5 f6 b3 e8 65 15 d5 e2 02 2a 5b 5e 6b 8f e2 09 51 1e d7 81 62 78 b7 6f 98 2c ec d9 4a fc ce 94 a6 6a 0c 79 b5 8b 5a 43 29 f8 83 55 95 6a 53 3c 0d 56 4c 0e f2 07 e5 99 72 06 f0 92 2b cc 82 ef Data Ascii: W^QJA25*TR^Wk)2ef@1B""alr[!W r5Y4B6KB2:cY*c7J&eYm15">g{UIS%[mN'9X#8EOXe,e*["kQbxo,JjyZC)UjS<VLr+
2022-07-01 14:30:01 UTC	532	IN	Data Raw: 81 c8 cb be 33 35 3d 02 5a bb 9a ad e0 ac 4e 81 30 1f 84 b6 c7 1a 5c 30 d1 46 ac be 20 2b 6d ee cf b4 a0 14 a7 14 f8 83 b5 ed c1 b3 bc c6 53 93 54 41 09 b9 c6 6b d4 98 77 35 8c 99 f7 c4 df 5a 6a b3 1f a5 ee 23 0b f2 38 b8 3b d1 f0 32 d6 0b e2 35 d9 86 8f da 76 2f 69 4e c2 06 7e f2 59 0f d3 9b e8 dc 94 2f fa 50 81 bf e1 06 46 05 ae 7c 4a 49 2e ae a9 bd 13 c8 f7 f1 17 32 b7 5b 98 84 8c 17 b5 a6 be 21 8b 73 55 be 25 4d 79 7b 44 dd a9 84 5f b4 1e 6f 52 b1 35 2a eb 46 a3 6c 73 e4 c1 2f 82 a7 66 89 96 2d d9 c4 05 33 75 46 ed 80 30 5f 16 e6 fd 65 22 a9 6c 5c 15 e0 db 2d ce 4a 1e b2 fa 94 7a a0 f2 8d 1a 3e 65 6f 5a d9 85 7e 60 5a 07 9d cb f1 50 68 d4 2b 85 b8 35 11 ca 2d ae 5a 5d 39 4c cd a4 37 05 98 27 09 b2 5c 16 f9 07 4c be 95 74 e6 07 20 79 75 9c 57 4b c3 b4 Data Ascii: 35=ZN0!0F +mSTAKw5Zj#8;25v/iN-Y/PFJl.2[!sU%My[D_gR5*F!s/f-3uFO_e"!lZ=eoZ~ ZPh+s-ZJ9L7!Lt yuWK
2022-07-01 14:30:01 UTC	536	IN	Data Raw: 43 f9 8d fb 23 91 9f 2d 42 67 9a 34 37 04 06 e6 bb 06 27 e2 40 ac 95 60 28 c7 83 b6 6e 0a 2d 6e d1 5b f1 35 f3 1a 15 7e bc 4e ba 94 2c fd ee 3b 5a 7f 72 c4 0b 70 1d b0 00 d6 65 b7 1f ef d6 52 ca f1 c4 3a 78 a8 0b 96 14 0c 18 6b ed 0b a0 7f 5d 66 a1 eb 5b 7f 99 84 64 62 e1 42 2d a2 fe de 26 b6 ac e1 95 b9 cc db 48 e3 b7 fa 44 77 4b 37 0c b4 bd e1 0e 5e b0 6f 41 88 ab 16 5b 8a 94 b4 73 2b 63 78 46 ad 0f 2e 21 69 7e b0 5a c1 5c 6e 60 d5 d7 fd b2 9b 4a 3d 24 cd 09 7b 94 eb 19 89 78 2f 14 15 a2 b2 83 1d 18 5b 2d 1d 25 30 b8 72 13 31 6a 2b 67 24 64 ab 3b 83 1a 2c 9c 39 07 1c 45 b4 3b 78 94 27 b1 cc cd c3 3a 90 b9 0c 18 71 32 74 d2 ef 90 c4 b0 27 00 53 b8 6e 2d 6c e2 18 ba 3a 73 05 77 c5 f2 71 2d aa 0e bb 9d 44 b5 6b 12 eb 4f bf 31 b2 af 7a 88 a8 74 fe 95 Data Ascii: C#-Bg47"@ ('n-[5~-N,ZrpeR:xk fdbB-&HDwK7^oA[s+cxF,!i-Z!n'}J4\$[x/[-%0rj+g\$d;9E;:x2t'Sn!l:swq-Dk O1zt

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	540	IN	Data Raw: b3 ba 3f bf c4 b8 3b 6d b4 3e 88 73 9e 95 0d 82 17 78 82 dd 8c 74 cc 57 e4 cc eb 51 e4 8e b0 e1 31 3a 22 ad 05 f7 88 36 30 c8 52 7b c0 ca dc b6 47 3c 81 94 d5 69 51 c0 3e f1 2a fa b8 80 bb d1 ed 15 a7 d2 31 b0 1c ba 4b 35 83 82 66 55 1d 39 80 b2 6a 9e 8e 2a 08 b2 ab 60 57 bc b4 08 0c 0e 91 0b e1 5d 4a 9b 68 1f 10 1c 83 d5 25 35 4c d1 c8 1e 8c 38 c3 c0 a6 56 86 9c 98 30 03 84 95 61 0a f7 d8 12 a9 40 0e 81 f9 84 1d 1d aa 01 5e 78 6d b8 02 00 eb 62 72 39 d2 5b b3 b1 9d e4 ca af de 81 8a 8e d6 87 88 ab 11 e9 fc c3 7d e4 87 b3 03 d2 e1 b4 01 29 0f 68 eb 38 bf 89 d6 7d 52 01 1d f9 17 58 67 99 ca cf 7d 6a 13 08 3b b9 9c 4b e5 92 fc 4a ad 93 34 4a ed 77 16 76 1d 16 be f0 f9 bf 88 37 0a 74 af fa 86 ae e1 e8 c4 23 b9 9d be cc c1 a8 ec fe d2 89 a4 6a bf de 31 Data Ascii: ?;m>sxtWQ1:"60R[G<iQ>*1K5fU9j*WJ]h%5L8V0a@^xmb9r[]A)h8M)RXGjj;KJ4Jww7t#j1
2022-07-01 14:30:01 UTC	544	IN	Data Raw: 6c 78 63 4d 0a c1 45 d1 e1 8d 92 72 57 b9 94 3c a6 6b 15 71 57 74 7b c5 6b 72 b8 f1 f7 16 3c 69 0b eb d8 a5 85 fc 11 17 09 8d 33 f3 2b a4 f7 9d c2 79 4a f3 28 95 db e9 52 bb 4a fa d9 d7 e8 26 78 ca d9 f4 35 fe 58 88 6f 5e 41 fb 60 f2 99 0c 5a 4e ae 8f fb 08 e4 47 59 fc 1f b8 95 29 c4 ff 00 2f 79 66 06 4b a6 a1 5a f5 9e 92 f3 46 38 2e 62 c2 f6 e9 8c fc 96 8e 78 b7 c4 49 c6 a8 57 5d e5 62 83 58 a2 58 d0 5d f7 23 19 37 25 f3 f9 95 de 55 c2 0a d8 b6 ac 7e 61 56 b9 e2 aa 17 ca 65 92 25 89 9b 77 f7 e9 2f d4 a7 4d d8 a1 46 98 74 7c dc b3 0f 3c b4 bf dd e6 8a 36 70 7d 22 0f 86 a8 38 81 23 48 bb 81 a0 d5 2b 6b 2a ae 02 8d 50 be 13 29 a0 6f 00 88 90 b9 e0 3b bb 77 95 70 25 39 9f 07 42 05 10 dc 22 5f d0 00 71 28 e2 04 ab 7b 8f be 3b ca f3 eb 2b 9a 85 d9 f3 32 e7 24 Data Ascii: lxcMERW<kqWt{kr<i3+yJ(RJ&x5Xo^A' ZNGY)/yfKZF8.bxlWjBxXj#7%U~aVe%w/MfT<6pj)"8#H+k*P)o;wp%9 B" _q({;+2\$
2022-07-01 14:30:01 UTC	547	IN	Data Raw: 6d be 9b 98 bf ab fe 18 fa d0 d0 c1 b9 77 ac dc aa dd fc 33 94 e7 70 2e 54 cd cb 71 28 6a 88 bd 61 d6 0a d4 77 4e c7 ad c7 ab 5c 76 83 7b 5e a4 a5 36 f9 25 90 1b 1c 66 1d 6d 63 74 e2 59 64 ea 01 98 5d d3 cc 47 41 88 b7 34 75 ce de 25 8b 9f 53 a8 f3 2a a2 f1 c7 a7 30 70 70 c5 c5 c6 a9 8b 8e e9 4c 5c 35 6e 21 15 67 91 2c 9d 4e 8b 7d 65 a0 63 49 af 6e 23 80 3e 68 f6 07 6f 76 7b b3 53 89 7d e2 9d 65 aa b6 45 65 91 37 88 9b ad 23 a4 c6 8b 66 a5 5f 33 00 bc 44 1c ca ee 99 7d 8c b4 bb 96 ed cb 2b 73 12 5d 2e 10 c4 1c 4b 97 31 d2 30 9d fe 88 22 a0 2f 73 10 05 a3 0b a8 02 c3 9a 4f 5b 69 87 97 44 d9 ce 20 13 82 f3 64 ed 04 69 1a 6a 33 5a ed 11 54 63 64 1a f4 59 89 06 47 25 73 1d 7c 8b 6b d6 73 40 af cb d5 87 33 c6 a9 c4 06 16 98 02 61 ec e6 65 87 2f 89 91 c5 c5 a5 Data Ascii: mw3p.Tq(jawNlv{^6%fmctYdJGA4u%S*OppL5n!g,N)ecIn#>hov{S}eEe73f_3D]+s].K10"/sO[iD diJ3ZTc dYG%\$ ks@3ae/
2022-07-01 14:30:01 UTC	551	IN	Data Raw: 07 f8 04 21 6d 1b 59 ba 63 fb 34 44 8b c6 36 fb 5f 5f 13 2f 66 b6 7e d0 4d 06 fb ee 2a df 6c 2a 64 25 b0 3a 61 85 3f 92 aa 6b 59 ec e9 16 96 8d 86 ce f2 e8 2d 4d 9a 94 55 89 a4 46 77 01 4a b1 45 dd 6a 38 aa 07 41 84 30 1d e3 88 da c6 47 43 52 e2 d0 8e aa 50 8a 07 de 55 b6 73 ea 45 97 56 74 26 30 6e e5 0e ef de 79 3d e6 2b 7e f9 78 dc 04 3f 66 3e 23 14 06 8f c7 ec 97 2e 53 83 e9 9d 79 25 a9 46 73 9e 2b e1 c4 2d 95 25 e5 98 07 50 cc 11 25 77 d2 21 bc 13 be 22 c2 d3 c0 ca ca 0d cf 81 76 7d 7e f2 80 2c 68 27 4a 97 62 b7 0c a2 3a 04 bb 57 0a b8 c0 9a 96 54 c8 76 79 9d 45 9d a0 f5 8a 69 18 59 8e 07 2f 99 5e 97 ac 00 50 30 28 e0 95 08 80 e4 e2 32 59 f7 4d 35 e8 30 e3 f5 4a 89 90 ef 63 e9 08 9a 90 6c f5 71 eb 0f 4d e0 ca 76 3e 4f 68 ac 27 33 94 60 97 50 63 33 8a Data Ascii: !mYc4D6__f~M^!d%:a?kY-MUFwJJE8A0GCRPUseVt&0ny=~-x?>#.Sy%Fs+~%P%w!~^v)~.h'Jb:WTvyEiY/^P O(2YM50JclqMv>Oh'3'Pc3
2022-07-01 14:30:01 UTC	556	IN	Data Raw: 9e 92 b7 67 f1 2e 9d 5e 65 40 00 26 ee 0c 65 57 1f 41 d3 99 97 7f 4e 25 54 31 df ea a9 47 d1 4a ce aa 0c 54 12 a2 de 4f 45 e0 94 26 71 96 f1 6f b1 1f f2 de 0f 4d fc 25 ef 8c 68 7c 0c 44 52 c9 43 22 f3 51 a0 85 c7 4d 7a 90 15 c6 f1 c4 07 46 ee e1 2c 7e f5 92 bc 81 ed 30 38 6b 98 1c de cf f3 11 96 6e df f3 e7 f2 2c 94 53 85 9f 69 81 25 db 10 d4 c9 5e a4 eb 68 67 84 4c 59 86 95 87 b1 7c bb 31 2c 1a 1f c4 e0 56 2e b1 cc 2c ba 07 6f da 60 a5 b7 3a 80 e9 05 f6 9c 0d e4 f0 8b 6e 04 e6 e5 9f 45 35 55 db ac 37 e2 51 57 d1 bb 81 d9 7b ad e6 2b 40 5f a6 71 ff 00 81 8f 94 a3 60 f7 88 9a ee cf 30 70 54 70 f5 84 10 b7 46 22 b5 de 4a a3 2f cc 58 16 df cc 0a 14 e3 13 ce a9 d7 98 ba af 1c 73 fa 86 19 4d 8e 84 71 0a 0a b2 3a 68 9e f7 01 b0 79 65 36 97 36 be 67 da a2 be d2 Data Ascii: g.^e@&eWAN%T1GJTOE&qm%hJDRC"QMzF,~08kn,Si%hglYl1,V.,o':nESU7QW{+@_q'OpTpF"J/ XsMq:hye66g
2022-07-01 14:30:01 UTC	560	IN	Data Raw: 98 ad 1c 99 50 b7 ce ef 35 2c 96 4d 58 7d ee 5c 02 a8 d5 4c 80 1c 23 7e cc 67 66 5a 2f 15 fb 86 76 8c 14 33 eb 1e 44 70 49 8e 6a e1 ac eb eb 33 97 e4 50 f4 2e a5 4b 58 a6 dc 78 18 aa a9 d5 1c 3a 53 31 79 85 61 39 31 a9 9e cb 99 f3 cf 97 eb e8 1e 60 c1 97 f4 d8 13 39 17 96 73 71 23 4f d0 6f 33 39 ed 0e 3e f3 96 4a 3e 6a bc 5d 40 56 1c 23 01 28 d3 b4 b0 3f 2f 4b 9b 12 7f d0 e5 97 b8 2d 14 08 85 1d d9 1e fa 7b 5c 25 33 70 65 e5 db 1f 36 89 f4 6e 32 56 3f 13 30 6a 0c c6 53 ed 32 72 27 44 b9 5a 3b 96 57 b0 38 24 1e 36 fb 22 8f d1 d5 3d 8d 04 a8 a1 5b 1d a6 94 5b b6 22 b6 6a a5 a5 d6 65 04 50 54 2d 25 77 26 1c c1 54 0c 2f 53 e8 05 1d e5 9b c0 3c e9 f3 2c 95 4c e4 f9 89 43 23 82 65 cf cd 18 3c 2c bc ee b1 fb 82 14 1d 0b ed 50 17 44 dd 04 71 f6 ef 1c e3 31 8c eb Data Ascii: P5,MXj]L#~gfZ/v3Dplj3P.KXx:S1ya91'ssq#Oo39>J>]]@V#(?/K-{%3pe6n2V0jS2r'DZ;W8\$6=[["jePT-%w&T/S<,LC#e<PDq1
2022-07-01 14:30:01 UTC	564	IN	Data Raw: 20 18 3c b0 7b 05 df 9e b5 f9 63 9c 4a f0 96 9d ba 3c a9 e8 8a 64 8e ea 0c fe 79 41 e6 f8 a4 a6 52 6f ba a5 66 dc 96 5a 44 46 8a 7d b2 e7 b0 59 7b 50 c8 2d ba 5b ae aa 1a 94 ef 0e 21 8b 0c 8b f5 d2 12 18 4a f9 6b 1a ba c0 81 43 b5 c8 37 23 5d e9 a4 24 aa 00 ff 00 c3 ba 40 2b 9a e3 a5 64 16 69 eb 64 d8 ee 8f 23 c3 7b fc 0d b0 5d b2 49 ad a6 9b a9 b6 09 63 81 7a 13 b3 a0 97 83 e7 b6 41 59 34 39 e4 34 24 76 67 72 b7 7f d5 82 6b 70 47 7e 12 c9 1a dc f0 27 7c 49 3e 25 b7 79 02 d4 14 34 92 a2 ab 86 06 bb d9 ef 02 e8 2e 8a 9a e1 be c1 e4 dd f4 50 24 d6 38 5d bc 7d f9 52 91 35 2e 19 0b 2e 21 94 9a 52 5e af 5e 11 47 18 34 b8 3a 11 82 c2 bc dd 4b d4 00 16 39 5c 9 92 14 ae e1 3b 58 08 29 a4 cb 65 b8 53 e2 12 4f cd b1 7d 3c d2 00 98 0d a2 a3 a8 b1 d0 fa 34 39 24 Data Ascii: <[c<dyARofZDF}Y{P-[lJkC7#j\$@>did#[lczAY494\$vgkrpG~ j >%y4.P\$8\$]]R5.!R^G4:K9\;eSO}<49\$
2022-07-01 14:30:01 UTC	568	IN	Data Raw: b1 b8 82 cb a5 d0 8c 3d c8 44 4d e9 01 63 cd 9f 2c 0c 82 17 7b 3c 5b 83 fb 74 46 41 29 b5 b2 6d a4 a1 8e 1b a3 10 9b b0 8c a6 49 db 4f 57 62 56 dd 0c b0 44 1d 4d e5 0d 67 18 2b 93 af 57 72 04 b7 87 72 90 c8 62 c1 bd 70 24 f3 bc 6d b6 bc 6f 19 09 b1 a3 cc 6c 46 b0 16 c0 41 3d ad 7c d9 f5 04 f3 c8 b2 f0 82 ce bc de 49 5b 38 f7 6e 42 ba 38 0f b6 7e d6 ce e3 5e f8 60 88 e8 cb 90 9b 69 f2 f0 84 13 a9 fe 43 c4 87 bd 84 5e bb bb 3a 86 06 c5 56 4b 65 9d f0 02 13 74 bd 58 42 5a de ad 65 56 5d 94 b7 a9 cd 99 b3 4b 65 3c 71 b7 9b 1b 13 f2 4a d9 27 b6 c9 63 92 7c 8c ce e2 0b ea d6 f8 84 f9 6c 2c ac 58 f9 66 ea 4f ec 0f d8 de 00 77 89 02 4d 01 03 e7 2d 67 89 7a 3a bb f9 2b 9e 2c 52 7a 61 37 b9 0f bb 7b 3e a6 4e 00 7d b4 25 b3 1e a1 1b ae 99 75 6d db dc be 25 3d b0 Data Ascii: =DMc,{<[fA)mIOWbVDMg+Wrr@bp\$molFA=?[8nB8~^iC^:VketXBZeVjKe<qJ'c ,XfOwM-gz+;Rza7{>N }%um%=
2022-07-01 14:30:01 UTC	572	IN	Data Raw: 1d e2 0d 79 9c 5a 62 2c b2 0f 0b 3c c1 fc 61 b2 4e ed bf c3 cc 89 0a 1f 7c 1c 5c 24 7a 82 44 fd 42 b3 35 4e bc 09 39 de 61 77 73 ea e0 26 3b b6 c6 04 d7 f5 1e f3 d7 fc 2e 2d 7c b5 f2 17 e5 c9 2c d9 7c bd 99 75 b3 48 67 83 1b 11 e2 35 0e 6c a1 e2 06 1c da 08 d7 a8 71 77 f2 1d 91 8c 12 58 ec b6 6f 90 bf 25 98 72 4f a8 3d c8 b4 90 7b 9c 17 76 43 66 f8 67 80 0f 02 5a f8 3b ea e4 e2 1e 36 17 84 a0 ba f7 2b ed a2 0f b9 0c 63 ce 4c da 75 62 d9 93 be 8b f4 87 8e e4 7d 9e 99 72 3a b5 a2 ca 2d fa df bc 05 a3 29 62 12 44 3c 09 65 98 b2 ce 22 d7 b2 37 6e 09 ca 7a a0 d7 59 76 0b 84 80 f7 6c 3a 4e fb 80 2d 4b 66 dd 8c 6d b6 52 6a bc 6a f7 e4 16 e5 33 2c b2 1c b9 58 0b 61 24 7a 98 fe 2d fc 95 80 a5 a6 42 6d f8 c0 5e 6d 7d 8e 7b 90 d8 98 61 61 33 af 76 f1 d5 ae 6c c4 02 43 Data Ascii: yZb,<aN\j\$DB5N9aws&.-, uuHg5lqwXo%rO={vCfGZ;6+cLubj;-)bD<e"7nzYvl:N-KfmRij3,Xa\$z-Bm^m{[aa3vC

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	576	IN	Data Raw: 2f 10 14 af 68 d0 f7 be 7a c2 f5 0d 2d d1 e4 14 47 ce f1 ef 76 4d 82 f7 06 8d f7 80 8e 14 32 1e 15 5a 3e e0 f9 b8 70 f1 65 46 dc 09 13 e1 32 85 d7 30 cd d3 01 2f 7a e1 b8 0e e3 a1 1c d3 b9 6b 8e be f1 da 14 78 0b 9e 04 12 f7 ce 01 2a 8c 22 7b 52 87 77 e3 de 40 7a 02 26 87 75 df e7 08 9d d1 20 34 f9 ec d5 e8 e7 07 bb 42 0b c2 7a 49 4f bd ef 17 00 d0 22 73 11 48 7a db 81 6f b2 e8 0f d0 79 39 42 f9 c3 d5 40 74 0e e1 2d 78 3e 77 8f 88 34 b4 ac 68 68 a8 8f 3c 65 e3 99 54 4b 78 6d f4 af 18 11 df 88 29 3a 44 7f 05 91 e7 24 40 4d c3 63 d5 9c 5e 1c cc a5 43 d3 80 ba f4 01 b5 ba 86 f2 aa 82 83 f0 06 4d ee c7 5c e1 7b ec 57 67 a4 f2 f0 3e 5c 24 7f ac bf f8 99 ff 00 a7 01 63 a8 82 22 78 45 30 2a 4a 4c 85 5b 28 e9 02 79 13 0b 2e 10 52 c6 48 0a d9 1f ef 01 08 91 a6 b6 c4 Data Ascii: /hz-GvM2Z>peF20/zkx*"[Rw@z&u 4BzIO"sHzoy9B@t-x>w4hh<eTKxm):D\$@Mc^ECbM\{Wg>\\$c"xEO*JL{[y. RH
2022-07-01 14:30:01 UTC	579	IN	Data Raw: 00 18 40 5a 31 80 3e 6b cf b3 8c 05 05 6a ae f9 39 c8 04 27 17 93 db f1 cd f4 b9 00 b1 11 5e c4 97 6e 7e d6 0c 0b 6a a3 cc 63 ee 88 e1 09 8e e5 34 85 7f c9 f7 80 a0 08 7c 52 3f 29 5d f9 30 b4 0d b5 3a d8 fa 74 3f 18 d6 cc 2a b8 5d 83 f6 8e 2b 74 a2 2f 64 a7 e7 6f b7 2e 53 be e5 5c 05 fa 55 f4 e5 e0 72 28 bd f2 4f 82 e1 14 e5 65 1c 95 50 fb 8f b3 06 5f 00 ec 92 d9 f2 53 f0 e2 09 23 4a 68 8c 9d de 4c 11 80 2e be a2 9f c0 3e b0 a3 03 13 80 ba f4 56 97 d9 9c aa 24 5d 5e 04 7d e9 fb c0 48 03 97 6a b5 3e 6d fb c3 dc 1b 2b c2 aa fd 0e 1f 74 c8 f2 7c fc 6d fc 62 4c 10 a8 e7 5f 83 5d ff 00 8c bf 8f 00 87 de ec f4 ff 00 bc a8 70 50 88 e9 55 0e bb d9 8c 72 4a 35 b0 9c 2d 34 e8 74 e3 17 bb 43 58 09 54 51 ae 9d 6b ce 13 8a d5 88 22 89 a0 76 48 69 40 70 f2 d6 50 dc 85 Data Ascii: @Z1>kj9^~jc4[R?]0:t?*)!t/do.SlUr(OeP_#_JhL.>V\$J^Hj>m+!tmbL_jpPurJ5-4tCXtQk"vHi@pP
2022-07-01 14:30:01 UTC	583	IN	Data Raw: b2 b9 d6 39 7d cc 59 7c 65 fc 7b cb eb 07 ef 16 13 07 de 57 83 ce 72 e4 c0 f0 50 9c 2b 48 6c dc 11 f5 8d 9b eb 6e 93 61 51 0a 29 b1 1c 1f c1 11 4f 30 42 bb 36 c3 de 4d fd 8c 23 7b 50 22 ad 57 ce 50 42 87 81 f9 c6 22 38 54 6f 5c e1 56 ab 0d ae f8 3d 86 07 d0 a1 a2 29 e5 ca a0 18 04 47 d7 e3 bc 5a ce bd ef 3b e5 4c 17 93 58 85 71 53 59 b4 3b e2 77 88 d8 10 01 78 28 af ad e0 76 90 d2 44 67 23 1e f8 32 0d 68 35 c6 f9 ea 5f 87 ce 48 d1 01 e0 e0 d1 3d 70 1f 6e 3c 2a 3e 59 d3 15 2f b3 ef 11 69 1d 9d 4a a0 dc 48 b4 60 48 70 2d 00 77 cc 0b e5 75 e0 30 89 f7 11 31 6f 40 53 ac ad 7a 74 16 ab 80 06 ab 03 cf 58 d3 e5 5f 21 43 82 08 22 f0 40 8b 56 32 74 a3 23 0b 0e 28 81 d8 36 9e f1 d5 14 d3 aa bd 82 e8 db cf 39 f0 22 2a 29 cd 7c 3c 60 7b 33 0d b7 22 ce 2c d6 6e Data Ascii: 9)Y[e{WrP+HlnaQ)O0B6M#{[P"WPB"8ToIV=A)GZ;LXqSY;wx(vDg#2h5_HApn<*>Y/iJH"Hp-wu0 1o@Sz4X_IC"@V2t#(69"*)< '{3",n
2022-07-01 14:30:01 UTC	588	IN	Data Raw: 00 d9 86 f7 6d 3e 80 f9 5c 2a 95 55 79 5b f9 ca e8 72 dc 40 75 f2 75 81 05 5b 8c 4b 28 4b 3c a8 72 bd ad 5e f2 1c 43 02 73 e3 2e 39 c4 ef 2f 8f d6 2b e3 2f c6 2c f4 60 ff 00 99 97 57 2d 30 6d c2 36 39 b9 22 13 e1 e3 e5 5d 19 ee b0 28 14 be fd 75 c7 58 b8 e2 e5 cb 97 ce 6d 79 cb e7 3c 57 c8 3e 01 ca fa 07 0c 88 20 32 17 55 69 da bb 7c 18 f1 e1 8c 7e 5f 1d fc 60 d5 89 a0 79 f6 eb 9e 30 b9 a2 35 f1 fe 7f de 31 a8 82 8f 3d e8 75 f3 88 08 f2 8a 6f 5b af 7e 71 92 cd d2 49 af 1e 19 e3 35 50 62 f8 96 3e 5e 72 59 ec 08 ec 78 45 d5 d6 cc 52 e0 d8 24 1d 24 d7 c1 86 e0 64 84 5e 78 8f 1d 6f b7 0c 24 48 76 41 6a e9 2e e9 b7 8c 5d 30 80 68 48 3b 1b f3 59 7d 3e f9 0b 5c 3c 5d cf 06 0b e8 be 96 4e 3f 4b 9b df 58 5c 77 26 05 70 31 81 77 9e 33 ed 72 d2 c3 07 2e c4 0e 04 a3 Data Ascii: m>!*Uy[r@uu[K(K<r^Cs.9/+/, 'W-0m69"](uXmy<W> 2Uij[_y051=uo[~ql5Pb>^rYxER\$sd\$xo\$HvAj;0jhH;Y)>\<]N?KXlw&p1w3r.
2022-07-01 14:30:01 UTC	592	IN	Data Raw: 17 b1 bd 64 0f 44 88 15 19 00 85 b8 09 55 53 69 25 a0 8d be 18 c0 e5 d6 b0 3e a4 c4 a1 c5 e6 c6 15 02 81 b8 a4 de ed 1b 76 17 8d 35 0d e9 17 91 a0 76 b4 e0 a0 26 93 05 5e 07 f1 6d 7f 3a fa cb 6f 28 8b d0 3e ac e3 03 b1 13 03 b4 13 8c 71 f0 20 f2 ac 9e a5 0f 9b 96 dd af f7 c3 24 d6 b1 d6 75 3d f7 f2 1a 3d 5a fa 31 29 3a 8b db b8 b8 3e 87 be 2e 69 1f 80 c4 02 87 0a d6 8e 99 88 d3 ca f9 14 16 ea 2a 9f c7 18 3a 52 0f 18 a9 d7 e3 36 04 4d 1f cb fe 3e b0 34 f7 ae f2 72 59 3c dc ec 2c 96 5a 9b c9 b7 5c f8 eb 2f ba 95 9b ca 5e f5 91 9a 18 05 37 4c 60 2d 09 2f 2c a7 d3 a9 56 ec 17 25 39 51 f7 a8 d3 47 32 0f d5 cb 4d f1 3c 70 b8 23 bd ca 5f 94 d5 f6 97 29 c6 3e d8 fb 60 dc 39 6f 07 e2 e0 ee e0 ef 9c 1e b9 f5 82 4e 7b c7 40 28 d8 f3 39 3e f8 c5 a5 eb d6 2f 8c 5d f3 Data Ascii: dDUSi%>v5v&^m:(>q \$u==Z1):+>.*:R6M>4NrY<,ZV^7L^-,/v9QG2M<p#_> 9oN@([>9/]
2022-07-01 14:30:01 UTC	596	IN	Data Raw: 0a 6e c8 fe c7 2e 6d c9 f7 8c 10 64 97 90 23 fa 5c 2e 35 a1 79 02 42 3c 63 11 a9 75 19 f4 26 be b1 0d 48 6a af b0 d6 fe f2 74 58 59 17 d3 38 fb c0 90 37 b8 2f 61 b9 f9 c1 80 0a 12 3f c9 3f bc 52 0f 9f fd e9 fe 70 24 c5 ba db a4 ba d7 de 4a 52 4d a5 fe 02 57 f3 92 0a e7 4b f7 26 ff 00 18 13 18 37 6a 4e a8 3f d6 4e 10 76 0f db 0a fe db eb 00 5a b7 40 1f 7d 97 f7 88 08 b8 ba 0f 98 a7 e0 c4 a3 7d b5 4f ae 7f 66 33 a1 9d 55 3e 59 aa 7e 72 e0 ca 46 2f c2 cd 7e 0c 40 79 95 09 fc cb f2 fd 62 02 5c a2 21 f5 a1 fa 1c 43 66 14 72 87 b5 34 fc 06 30 11 8b a0 b1 0a aa 84 a7 c6 35 25 00 47 a9 62 8f 9a fb cd 5e e9 00 5e 14 00 bd a9 1f 13 2f 25 dc 3a b5 c6 92 59 c1 e8 c6 81 1d ae 51 a2 34 f9 21 96 5e 60 a6 22 5a a1 2f b9 ce 14 28 51 a7 36 b0 17 a7 9d 6f 08 26 54 13 75 52 Data Ascii: n.md#l.5yB<cu&HjtXy87/a??Rp\$JRMWK&7]N?NvZ@[]Of3U>Y-rf/~@yblCfr405%Gb^%/:YQ4!^"/(Q6o&TuR
2022-07-01 14:30:01 UTC	600	IN	Data Raw: 0c 54 18 e2 c4 0c 39 67 33 dc 8c 02 08 21 36 86 95 08 77 2e 5e 61 db 68 e8 1c 21 55 8b 13 25 8a 91 30 36 e4 55 16 54 54 c7 cd 74 c9 e3 b6 22 26 82 0c 11 02 32 45 34 af 37 5f 5a 98 45 6d 77 a3 47 b5 eb 12 73 32 a5 01 c2 fa e1 99 5c e1 34 a4 6e c3 85 d6 ad df 58 c9 3b 31 27 60 1d 4c d7 39 4a 84 b0 f7 fc 38 58 a4 fa 50 81 af 4a 3f 58 94 94 ae 9b 03 11 fb 1c 40 f1 a7 07 69 ef 35 df 3e 70 53 8e 30 eb d9 86 ac e2 4f 9c 7a af 78 c3 df 97 2f b3 fc e1 97 8e 78 e3 39 83 f9 c0 fc 61 e4 f3 87 f3 85 de b7 87 35 4c 88 74 65 4e ef c6 4b c0 15 e8 19 f3 f3 75 85 6f 84 47 a5 03 f8 c7 90 86 91 d1 22 02 8d 2a 68 eb 93 0a 25 ae b1 8d 2d 4d a1 66 aa 5d f8 c2 0b cd ec 36 a8 b2 a0 1f 38 18 dc b8 42 69 14 77 b1 de 38 d6 ba 1d f7 77 0c 92 9e 14 6f ad 6b 39 80 b9 05 fe f0 00 e3 Data Ascii: T9g3!6w.^ahlU%06UTTt"&2E47_ZEmwGs2!4nX;1/'L9J8XPJ?X@i>p5SOOzx/x9a5LteNkUoG*"^h%-Mfj68Biw8wok9
2022-07-01 14:30:01 UTC	604	IN	Data Raw: 8c 24 0b 53 9b 5d d1 ab eb c6 23 ab 00 19 f9 8c 77 ea e1 43 00 1a 01 db b7 6d b8 a5 60 67 05 75 d6 f7 90 da c0 45 1b ba d8 88 37 d6 12 5a 83 90 02 1d 7e e5 e3 0e 65 7e 30 1f 37 1e 89 f2 19 34 a2 08 72 1e 83 35 b7 ba e7 da 1f ad 83 f4 c5 97 a5 ba 60 70 21 4d 83 57 c6 25 80 9a 56 42 f8 6a 92 2b c6 28 cc e1 0a c7 10 a7 6a 8d 17 8c 8a 7b b5 60 9a 77 51 45 04 62 30 70 88 d8 20 c0 06 80 00 40 e0 e0 cd 0c 04 78 2a 8f 7e b9 de 0b 11 53 4c 3c f6 eb 26 2d ec 7c 1e 31 81 e1 36 40 df 9b 91 11 00 e9 59 db ce 4c 80 30 10 ab ed e0 ff 00 ee 4f 24 c4 08 6b 6b c2 ce 07 0c 41 20 dc 02 72 07 3a fe 71 e4 61 52 18 7a 3a cf f2 67 10 03 6d 94 79 09 cf 74 ae 52 52 65 42 2b a8 96 2e fe b2 d8 0b 68 23 ec df 26 06 16 ea a5 1f c7 53 0e fb 29 88 a4 7b 5f 5b c3 a6 00 a5 4b ea ca 13 f3 Data Ascii: \$Sj#wCm`guE7Z~e~074r5`p!MW%VBj+([(`wQEb0p @x*~SL<&~ 16@YLOO\$kkA:rqaRz4gmytRRReB+.h#&S)[_ [K
2022-07-01 14:30:01 UTC	608	IN	Data Raw: 1c eb 8f be 30 b0 53 48 28 b0 d9 d8 68 4f bf 39 6d 52 a0 4d 5d 73 e5 f6 7b c5 4e a6 c0 c2 f0 09 02 68 bb 99 70 dd 19 45 2f 72 dd 74 07 bc 08 a2 21 d5 3a 4f d4 f9 73 6b 58 6e 5c 48 9a d6 fd 4c 48 0d c2 00 54 da bb 3c 6f f7 84 00 35 51 05 07 c3 9d 71 ab f1 83 2f 9d b6 e1 0a ef 97 e3 ef 26 cc 82 c0 5b b5 75 cc 0e 57 f3 83 c5 41 fb 23 fb 3f 78 ff 00 41 f7 a7 f6 63 ce 2e 0c 7c dd fd e2 1b 34 97 fe 7e 33 7a 77 c2 ec ab 8b 40 76 28 89 18 42 2a 1f 9c 49 77 52 92 a1 5a 46 35 2c f4 e4 f5 b9 74 9e 19 1d 80 d8 e9 6e f5 87 2a 84 89 c2 d0 76 f3 f7 bc e3 f4 4a ba 02 7f ac 36 c4 82 a5 17 96 1b 79 ea e1 3a 04 21 81 15 23 d2 47 67 58 7b 3a 52 3a 2d b5 35 ad 5f e3 0c 9a d6 85 23 a3 b6 af 55 5b ab 85 a5 32 0b 60 0a 34 45 01 95 69 70 00 18 74 ce d2 a2 35 ba 0e f6 5c d3 15 89 Data Ascii: 0SH(hO9mR)s{NhpE/rt!OskXn\HLHT<o5Qq&[uWA#?xAc. 4~3zw@v(B*lwRZF5,tn^vJ6y;:!#GgX{R:-5_#U [2'4Eipt5\

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	611	IN	Data Raw: 0e 70 55 81 b6 03 f8 e7 f5 95 0f e8 16 1d 03 37 f7 8c 11 38 48 d7 6a 85 f6 b0 82 24 54 09 2f 9b 1f ac a6 8f ac 04 3c 46 fb 89 88 99 4b 2a 10 52 c5 0d 1a e3 46 56 12 bc 93 bf 78 e0 58 3b 51 2e 5b 0d 09 4f 18 c4 4c ca 43 f3 95 6c 9a 7f ac 2d cd ce 4c dc c4 77 bc 89 ce 4f 66 4d 9c 60 b2 41 86 ab 94 75 cb 3f d6 23 39 2b c4 5d f9 98 c2 91 e5 15 71 64 59 f0 a3 f0 7b 3f 78 44 00 86 91 77 ae fa d6 0f ed 8e 17 91 95 7f f9 86 42 52 12 d6 33 40 71 dd df 26 35 9e 02 48 76 2e c9 c7 03 86 98 8d 14 a5 85 b0 06 75 bc 20 6f 37 4d 46 08 9c 0d 9f 5b ca 4b 41 f0 af 17 b7 d3 30 23 0c a5 97 5a b4 41 21 a0 f3 bd e3 bc 00 10 3d 08 f3 78 2d ec c6 66 ea 0b 09 14 3c 9c 91 e1 30 dd 68 60 ca 58 f6 97 fb c3 4d 00 25 10 46 35 5d 69 10 39 c6 10 4b 44 83 56 01 a3 7c 7b 33 61 56 d2 Data Ascii: pU78Hj\$T/<FK*RFVxX;Q.[OLCI-LwOfm'Au?#9+JqdY{?xDwBR3@q&5Hv.u o7MF[SA0#ZAI=x-f<0h'XM%F5]j9 KDv)[{3aV
2022-07-01 14:30:01 UTC	615	IN	Data Raw: af 18 13 dd 2a e8 51 e0 67 f0 f7 8c 2d 02 8a 42 f4 9e 12 6b 0a 26 d5 5b 37 b0 08 91 d9 44 eb 1e 2c 27 3c 68 28 d4 ba 74 98 fb 5a a3 bc 4a 4a 26 d7 8d fe 72 9c c4 b2 d8 66 de 0d 42 26 ba c4 0d c2 29 c5 2a 53 80 7d ce 31 81 a8 49 66 cd c6 f0 78 ae 2a bc 82 2a 3c f7 a1 eb 46 1c d3 06 81 83 1e 18 bb 61 39 ed b8 4a 08 52 45 71 01 90 f2 43 7e 4c 70 86 a9 54 56 82 28 4d 7f 38 cc 6d 05 01 d9 44 88 f5 e1 c3 d4 42 c8 05 e8 db af 0e 5c a4 16 b4 e3 48 68 6b ba 5b 9a 78 ba 51 3d 8c 05 e0 de 17 00 0a 5a 46 c0 7b 35 75 b9 93 67 f4 10 42 8a 28 1e 1b b1 1c a4 b9 c8 f0 10 a5 78 95 d9 bc 6a 19 56 22 b6 aa 4c 6f 2e 14 90 34 5f b3 66 dd 56 e3 48 05 34 d0 f2 03 0e 23 8a 65 02 22 64 e6 2a 4e 37 eb 07 70 ad 55 ad 02 21 fa 70 13 6a 25 45 2d 68 20 77 32 63 23 a0 31 0d 26 89 d4 df Data Ascii: *Qg-Bk&[7D,'<h(tZJJ&rfB&)*S]1lfx**<Fa9JREqC-LpTV(M8mDB\Hhk[xQ=ZF(5ugB(xjV"Lo.4_fVH4#e"d" N7pU!p]%)E-h w2c#1&
2022-07-01 14:30:01 UTC	620	IN	Data Raw: 38 e3 1d 2e 00 1a 13 a9 76 6d f1 e7 0b 68 01 00 d2 ed 0f 64 b8 d3 42 86 80 56 34 13 9f 26 a6 2e 5b 1d 3b 24 a2 58 77 cc b8 65 8a 50 24 f2 a2 2b c3 41 4c d0 1a 13 80 bd a8 09 0e 27 19 56 dc 71 90 d8 1a 63 d2 17 e3 1a aa 85 2a e2 04 1a f0 72 65 7a 42 93 98 6d 5b 18 f7 2e 78 f2 34 9c 39 17 7d df 79 72 5b 96 0a 1d 01 77 27 01 bc 81 40 60 36 7b 68 22 47 f9 c9 9d 64 08 09 a5 0e 44 e5 f1 f1 8d f1 5a 1c 49 48 f2 89 a1 12 66 ba 00 50 f0 7e 6c 34 c8 f1 e7 1e 8d 4a 2f 0e 1a 1c 6c 17 be 9d 64 2f 09 a0 55 ce aa d7 c6 72 92 d1 f0 5d c0 8a b7 ce 1a 54 aa e4 03 91 0d ae 20 1d 90 be 46 a8 a7 89 4e 31 00 08 84 00 84 27 1d 38 8d 20 29 5d 0c 37 bc 34 93 c8 10 b2 a3 a4 3a 63 79 42 06 20 d5 ac 02 e8 8b bd e3 d1 96 8d 60 25 61 ec f1 5c 5e 01 40 5d 75 1b d3 8b 3a cb ea d1 71 66 Data Ascii: 8.vmhdbV4&.[;\$XweP\$+AL`Vqc*rezBm[,x49]yr[w@'6[h"GdDZHfP-l4J/lD/UrJT FN18'']74:cyB `%a^@ @:qf
2022-07-01 14:30:01 UTC	624	IN	Data Raw: 49 b0 c0 ca ce 5b 0d 92 90 05 a9 f1 8d 5a 02 23 7e d5 03 bd df 8c 40 2e 09 0d 2b 64 a5 59 f1 82 0d 50 ec 0d 22 02 ef 73 73 d4 cd 78 c6 f8 32 ca 56 37 5a a1 cf 58 58 74 00 25 10 db 2c bd 09 d6 32 33 9e 70 22 31 00 09 a4 bb f2 e1 d0 ed 0a 20 a9 51 2a b2 cf c5 c0 71 03 bb 90 02 6c 02 a6 89 ac 05 b8 bb c9 41 68 88 ec 36 3d a2 8d f3 68 ee 87 02 c6 86 0c e4 31 ca 51 09 a3 b0 35 d5 0b ae d7 10 30 48 b0 85 17 5e 44 9e 32 f2 23 4a 35 5f 4e 8e 3c 61 28 49 dd 10 17 84 de b3 4c 4a 20 79 00 9e 95 b7 bc 4a df 91 4b 29 e4 70 4f 79 6a c2 58 60 0d e8 82 26 8f 06 38 7b 70 91 ef 8c 8b 5e a4 af 7e 94 33 2c aa d7 9d 1f 3c 66 73 70 6c 4c f8 d5 fe 30 00 3d df 26 7f 6c 1a c3 f1 18 14 21 54 e7 08 74 4e 2f 80 c1 d5 49 4d f3 9c 3c 08 a1 8b ba 51 51 13 82 eb 08 2e 90 77 f6 27 31 f1 Data Ascii: l Z#~@.~+dYP"ssx2V7ZXxt%,23p"1 Q*qIAh6=h1Q50H^D2#J5_N<a(IPLJ yJK)pOyIX`&8[p^~3,<fslpL0=&l ITn\IM<QQ.w1
2022-07-01 14:30:01 UTC	628	IN	Data Raw: b7 fa c2 e1 1a 00 b1 ae 16 6e 6c e7 bc 8f 25 74 0b 7c 83 73 e3 0b 24 b3 44 ac f2 20 eb 8c d6 5a 62 4e f8 b6 c7 ec e3 10 2c d0 2e f4 38 d4 27 78 06 c8 12 08 bb 1d c6 72 38 92 3b a0 40 d0 c5 17 eb 22 28 5c 10 ec 0c 2c be 13 0b 79 0d 44 8d 50 68 0e 43 5c 61 6f d1 19 bf 83 44 1e 22 14 d7 8c 75 0b 01 54 44 6a 72 27 11 77 be 38 c9 f6 00 2c a9 da 1a 0a 6d 9e 93 8c 7c d7 1d 8a 22 16 35 96 51 3c 38 e0 eb b0 4b 5e 34 a6 fa 4e f5 96 14 b4 02 3e 98 68 e1 f9 c5 40 b8 c2 2b 42 da bc 43 c6 f0 25 85 ca f8 01 8a 87 c7 c6 4f 35 53 40 f3 3e 1b af c6 70 48 60 d1 e2 85 93 ea e0 1a 91 e5 83 3a 00 92 cd 60 42 86 d2 23 7d 85 1b f5 d6 15 68 3a b1 35 9a 43 cd a7 3d e3 f0 c9 a2 e3 c5 29 af 12 eb 08 88 1a 80 4d ba 79 13 83 79 bf 73 14 37 49 b1 ea bf 1a c4 31 fa 11 03 10 d8 5d 93 bc Data Ascii: nl%t s\$D ZbN,.8xr8;@("(\,yDPHc\aoD"uTDj)r#w8,m "5Q<8K^4N>h@+BC%05S@>pH`:"B#j:5C=)Myys7l1]
2022-07-01 14:30:01 UTC	632	IN	Data Raw: a0 10 05 9f 83 ce 4b 67 4c 05 36 7e 72 5a 50 74 4d 1f 78 4d 85 36 35 9d 72 24 7e 93 0e 8f ae 44 0c e7 41 fa c4 16 c4 16 88 ff 00 9f bc dc b7 d9 38 6c 50 8f c3 80 17 c0 68 00 ec 40 53 8f 78 95 78 a1 a2 df 2a f2 b4 d5 bc 82 34 83 5e d1 a1 59 37 d1 93 69 10 04 27 08 08 0d fc 6b 01 07 2e b4 47 ce 87 5e 74 6f 29 bc 2a b2 41 78 1a bc e1 da 10 03 55 f5 e1 ef 0e 68 db 22 06 d1 08 9d 71 82 b5 21 a4 5a e9 5a dd e7 1c 81 31 8a 47 62 8f c7 1b 32 7c 42 97 10 83 d4 67 af de 12 50 28 e0 53 a4 8e 9e b9 f7 9c e4 c3 21 5a a1 05 ab 75 c1 c2 e3 6c 45 0c a1 5a 80 6a 7c 33 5b cd c0 2d d8 89 74 22 1f 06 17 29 01 2d 84 75 b9 d7 3d 61 6c cc 2a 15 b4 09 2f 3a f3 82 55 08 01 0e f6 8c a7 2d 8b f9 c6 5d 68 58 8e 40 c5 df bd 64 f4 16 01 f2 1a 15 53 b8 61 d5 ea 4c e1 b1 d8 23 ee bf 8c Data Ascii: KgL6~rZPTmXm65\$~-DA8lPh@Sxx^4^Y7i'k.G^to)*AxUh"q ZZ1Gb2[BgP(S!ZuIEZj]3[-t]-u=al^*/:J-hX@dSaL#
2022-07-01 14:30:01 UTC	643	IN	Data Raw: ea ae 01 52 8c 15 ae 99 a0 03 bd 82 ea 02 0a 1a 68 e0 0d c4 a3 ad c4 aa 00 04 39 08 e5 c1 52 dd b2 a6 98 02 b0 38 08 43 39 ea 8a 0e 8c 83 00 0e b4 1c b1 ca 5c 20 9a 9d 4a 92 bc 8a ab da 45 47 2b 6a f0 a0 53 40 16 8e 6a 0c df 87 df ac 10 26 33 8f 2f ce 3e 50 18 45 9b c4 50 14 6d 09 b5 c2 95 cf 5a 75 e6 b8 73 6e 5a 7b eb 01 34 25 a2 ba 0c 94 5d 4f 3e fb fc e2 56 85 3a 36 7d e3 41 a5 57 de 6f 43 ab cf 3f 79 35 78 73 be ae c4 d2 9f 1b 32 9e 06 39 0e b0 8e c1 aa 33 9c 60 08 07 49 d1 8c 08 ba f4 c7 61 b3 78 d7 9c 0d 48 2a 31 9c 45 0b 7b e6 79 98 87 cd 20 03 0d 85 02 9c e8 29 de 32 03 23 0b c3 59 05 eb 4f d6 33 ec ab 9a 50 a8 82 6e 9b 74 79 d6 1e aa b0 88 3d 88 a0 38 39 1f 7d e1 1a 88 56 ce f4 80 42 b 6 31 bc 63 7f 68 5c 11 2a db 83 80 9d e3 16 55 db a3 6f 28 50 4f Data Ascii: Rh9R8C9\ JEG+JS@j&3/>PEPmZusnZ{4%}O>V:6)AWoC?y5xslN93`laxH^1E{y }2#YQ3Pnty=89)VB1chl^Uo(PO
2022-07-01 14:30:01 UTC	659	IN	Data Raw: e5 fc e3 21 09 4e 4d e0 1a 3a e0 fd 6b 10 2e c8 e0 1a 68 1d 4f 9e 70 26 79 76 79 7f ef bc b2 ca 43 5e 0c da 42 8d d4 3d e1 28 83 04 d5 f6 e3 04 49 cf 20 fb df f3 9c 88 ae 69 de 29 1b 51 9b c4 4d ab 78 f5 80 7b 9b dd db eb 37 36 14 8a d6 72 7e 71 02 a4 70 2e f8 94 06 fe a3 81 5a 50 1f b0 7d 78 de 08 05 00 10 30 9a 5b 27 9d eb d5 cb 06 6b c7 99 b9 e2 1f e7 06 8c 1a bb a2 29 b0 44 2f 79 bc 56 e1 0a 88 8e b4 13 f4 c1 e2 62 bf 3f 78 70 e3 c7 fe 7c 63 95 09 8f 1e 31 3f 18 9b 75 81 1e 30 c9 e7 27 58 9a 75 93 f3 f3 93 f3 32 7a c3 08 8e b5 82 00 a6 bf 05 cd 3e 6f d5 c7 40 50 f0 61 00 da 30 7d b3 01 18 07 79 56 51 e1 e7 80 30 ad 1c d0 0e e4 2a 27 6a fc 60 a7 81 e4 a0 6a d8 6a 31 0b c5 cd b1 0c a4 05 0e c2 bb eb d1 ce 31 a0 a4 12 29 76 f4 bc 3a 78 d6 3a 2d a0 4f 65 Data Ascii: !NM:k.hOp&vyvC^B=(l)l)QMx{76r~qp.ZP}x0[k]D/yVvb?p c1?u0'Xu2z>o(Pa0)yvQ0"}j11)vx:-Oe
2022-07-01 14:30:02 UTC	675	IN	Data Raw: ca bb c3 05 4c 19 b2 c1 f9 c8 5e 20 6e ba fa c7 a3 ef 99 80 0d b6 f4 ff 00 79 2a c8 f5 dd c5 54 af 98 f1 f2 62 6a ad f9 88 fb c2 d0 49 da 37 16 ec 4e f2 ed 40 e8 2e 10 81 53 a3 84 c6 14 46 f0 64 5e 77 ef 35 2a fb c4 28 6a cb ad 63 15 ba 2d 73 7b 45 a4 8a 1a 57 20 f3 1b 49 53 8c 26 46 00 0a 1a 00 35 0f 06 12 4c d7 82 62 6f c6 04 6b 6b 98 91 34 8a 9b eb c7 78 85 40 58 02 8e 36 09 72 72 5c b4 02 a8 40 36 ad e8 2a 86 78 92 e3 03 be 01 77 3a 38 c5 85 a5 37 39 ea ad e1 95 6a f0 e2 39 87 3f 39 b1 25 c4 2f e6 47 25 0f 6a 00 eb d8 5f 16 63 8a 96 9a 73 ed b8 72 67 9b 16 4d 29 3f 04 30 02 35 b7 5c f6 8b 57 c6 72 ae 22 3d f5 8b 49 68 22 72 fe 68 71 92 c0 5d 35 08 f9 47 9c 86 21 e8 88 47 11 93 e3 1d c4 34 1d f9 7f d7 f3 8f 4f d6 7e 45 f1 31 f0 00 70 36 7c 3c 8f c6 19 Data Ascii: L^ ny*TbjI7N@.SFd^w5*(jc-s{EW IS&F5Lbokk4x@X6rr(\@6*xw:879j9?9%/G%[_csrgM)?05lWr~=lh^rhqj 5GIG4O~E1p6]<

[illegible]

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49844	69.49.244.155	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:04 UTC	711	OUT	GET /payment/frontend_paper_lantern/images/office3651.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: eyecandyashcompany.com
2022-07-01 14:30:04 UTC	712	IN	HTTP/1.1 200 OK Date: Fri, 01 Jul 2022 14:30:03 GMT Server: Apache Last-Modified: Sat, 18 Jan 2020 17:50:20 GMT Accept-Ranges: bytes Content-Length: 18147 Connection: close Content-Type: image/png
2022-07-01 14:30:04 UTC	712	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 0d 49 48 44 52 00 00 00 bb 00 00 00 bc 08 06 00 00 00 20 95 df d2 00 00 00 20 63 48 52 4d 00 00 7a 26 00 00 80 84 00 00 fa 00 00 00 80 e8 00 00 75 30 00 00 ea 60 00 00 3a 98 00 00 17 70 9c ba 51 3c 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 7 3 00 00 0b 13 00 00 0b 13 01 00 9a 9c 18 00 00 3a ee 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb ff 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 0a 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d Data Ascii: PNGiHDR cHRMz&u0` :pQ<sRGBgAMAapHYs:iTXtXML:com.adobe.xmp<?xpacket begin="" id="" W5M0MpCe hiHzeSzNTczkc9d"?><x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmpk=

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:44 UTC	753	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body><h1>Not Found</h1><p>The requested URL was not found on this server.</p><p>Additionally, a 404 Not Found error was encountered while trying to use

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49912	69.49.244.155	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:46 UTC	754	OUT	GET /payment/frontend_paper_lantern/images/gmail.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: eyecandylashcompany.com
2022-07-01 14:30:47 UTC	754	IN	HTTP/1.1 404 Not Found Date: Fri, 01 Jul 2022 14:30:46 GMT Server: Apache Content-Length: 315 Connection: close Content-Type: text/html; charset=iso-8859-1
2022-07-01 14:30:47 UTC	754	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body><h1>Not Found</h1><p>The requested URL was not found on this server.</p><p>Additionally, a 404 Not Found error was encountered while trying to use

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49808	69.49.244.155	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:00 UTC	1	OUT	GET /payment/frontend_paper_lantern/index.html HTTP/1.1 Host: eyecandylashcompany.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-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-07-01 14:30:00 UTC	5	IN	HTTP/1.1 200 OK Date: Fri, 01 Jul 2022 14:29:59 GMT Server: Apache Last-Modified: Thu, 29 Jul 2021 07:13:16 GMT Accept-Ranges: bytes Content-Length: 21845 Connection: close Content-Type: text/html

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:47 UTC	755	OUT	GET /payment/frontend_paper_lantern/images/gmail.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: eyecandylashcompany.com
2022-07-01 14:30:47 UTC	755	IN	HTTP/1.1 404 Not Found Date: Fri, 01 Jul 2022 14:30:46 GMT Server: Apache Content-Length: 315 Connection: close Content-Type: text/html; charset=iso-8859-1
2022-07-01 14:30:47 UTC	755	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 3a 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body><h1>Not Found</h1><p>The requested URL was not found on this server.</p><p>Additionally, a 404 Not Found error was encountered while trying to use

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49809	69.49.244.155	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	13	OUT	GET /payment/frontend_paper_lantern/css/hover.css HTTP/1.1 Host: eyecandylashcompany.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://eyecandylashcompany.com/payment/frontend_paper_lantern/index.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-07-01 14:30:01 UTC	86	IN	HTTP/1.1 200 OK Date: Fri, 01 Jul 2022 14:30:00 GMT Server: Apache Last-Modified: Mon, 11 Jun 2018 09:44:34 GMT Accept-Ranges: bytes Content-Length: 114697 Connection: close Content-Type: text/css
2022-07-01 14:30:01 UTC	86	IN	Data Raw: 2f 2a 21 0a 20 2a 20 48 6f 76 65 72 2e 63 73 73 20 28 68 74 74 70 3a 2f 2f 69 61 6e 6c 75 6e 6e 2e 67 69 74 68 75 62 2e 69 6f 2f 48 6f 76 65 72 2f 29 0a 20 2a 20 56 65 72 73 69 6f 6e 3a 20 32 2e 33 2e 32 0a 20 2a 20 41 75 74 68 6f 72 3a 20 49 61 6e 20 4c 75 6e 6e 20 40 49 61 6e 4c 75 6e 6e 0a 20 2a 20 41 75 74 68 6f 72 20 55 52 4c 3a 20 68 74 74 70 3a 2f 2f 69 61 6e 6c 75 6e 6e 2e 63 6f 2e 75 6b 2f 0a 20 2a 20 47 69 74 68 75 62 3a 20 68 74 74 70 73 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 49 61 6e 4c 75 6e 6e 2f 48 6f 76 65 72 0a 0a 20 2a 20 48 6f 76 65 72 2e 63 73 73 20 43 6f 70 79 72 69 67 68 74 20 49 61 6e 20 4c 75 6e 6e 20 32 30 31 37 2e 20 47 65 6e 65 72 61 74 65 64 20 77 69 74 68 20 53 61 73 73 2e 0a 20 2a 2f 0a 2f 2a 20 32 44 20 54 52 41 4e 53 49 Data Ascii: /* * Hover.css (http://ianlunn.github.io/Hover/) * Version: 2.3.2 * Author: Ian Lunn @IanLunn * Author URL: http://ianlunn.co.uk/ * Github: https://github.com/IanLunn/Hover * Hover.css Copyright Ian Lunn 2017. Generated with Sass. */* 2D TRANSI
2022-07-01 14:30:01 UTC	178	IN	Data Raw: 74 69 6f 6e 3a 20 30 2e 33 73 3b 0a 20 20 74 72 61 6e 73 69 74 69 6f 6e 2d 64 75 72 61 74 69 6f 6e 3a 20 30 2e 33 73 3b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 69 74 69 6f 6e 2d 70 72 6f 70 65 72 74 79 3a 20 74 72 61 6e 73 66 6f 72 6d 3b 0a 20 74 72 61 6e 73 69 74 69 6f 6e 2d 70 72 6f 70 65 72 74 79 3a 20 74 72 61 6e 73 66 6f 72 6d 3b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 69 74 69 6f 6e 2d 74 69 6d 69 6e 67 2d 66 75 6e 63 74 69 6f 6e 3a 20 65 61 73 65 6d 6f 75 74 3b 0a 20 20 74 72 61 6e 73 69 74 69 6f 6e 2d 74 69 6d 69 6e 67 2d 66 75 6e 63 74 69 6f 6e 3a 20 65 61 73 65 2d 6f 75 74 3b 0a 7d 0a 2e 68 76 72 2d 66 6c 6f 61 74 3a 68 6f 76 65 72 2c 20 2e 68 76 72 2d 66 6c 6f 61 74 3a 66 6f 63 75 73 2c 20 2e 68 76 72 2d 66 6c 6f 61 74 3a 61 Data Ascii: tion: 0.3s; transition-duration: 0.3s; -webkit-transition-property: transform; transition-property: transform; -webkit-transition-timing-function: ease-out; transition-timing-function: ease-out;}.hvr-float: hover, .hvr-float: focus, .hvr-float: a
2022-07-01 14:30:01 UTC	186	IN	Data Raw: 58 28 2d 32 70 78 29 3b 0a 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 58 28 2d 32 70 78 29 3b 0a 20 20 7d 0a 20 20 38 33 2e 32 35 25 20 7b 0a 20 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 58 28 31 70 78 29 3b 0a 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 58 28 31 70 78 29 3b 0a 20 20 7d 0a 20 20 31 30 30 25 20 7b 0a 20 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 58 28 31 70 78 29 3b 0a 20 20 7d 0a 20 20 7d 0a 40 6b 65 79 66 72 61 6d 65 73 20 68 76 72 2d 77 6f 62 62 6c 65 2d 68 6f 72 69 7a 6f 6e 74 61 6c 20 7b 0a 20 20 31 36 Data Ascii: X(-2px); transform: translateX(-2px); } 83.25% { -webkit-transform: translateX(1px); transform: tanslateX(1px); } 100% { -webkit-transform: translateX(0); transform: translateX(0); }@keyframes hvr-wobble-horizontal { 16

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	194	IN	Data Raw: 20 70 65 72 73 70 65 63 74 69 76 65 28 31 70 78 29 20 74 72 61 6e 73 6c 61 74 65 5a 28 30 29 3b 0a 20 20 62 6f 78 2d 73 68 61 64 6f 77 3a 20 30 20 30 20 31 70 78 20 72 67 62 61 28 30 2c 20 30 2c 20 30 2c 20 30 29 3b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 2d 6f 72 69 67 69 6e 3a 20 31 30 30 25 20 30 3b 0a 20 20 74 72 6 1 6e 73 66 6f 72 6d 2d 6f 72 69 67 69 6e 3a 20 31 30 30 25 20 30 3b 0a 7d 0a 2e 68 76 72 2d 77 6f 62 62 6c 65 2d 62 6f 7 4 74 6f 6d 3a 68 6f 76 65 72 2c 20 2e 68 76 72 2d 77 6f 62 62 6c 65 2d 62 6f 74 74 6f 6d 3a 66 6f 63 75 73 2c 20 2e 68 76 72 2d 77 6f 62 62 6c 65 2d 62 6f 74 74 6f 6d 3a 61 63 74 69 76 65 20 7b 0a 20 20 2d 77 65 62 6b 69 74 2d 61 6e 69 6d 6 1 74 69 6f 6e 2d 6e 61 6d 65 3a 20 68 76 72 2d 77 6f 62 62 6c 65 Data Ascii: perspective(1px) translateZ(0); box-shadow: 0 0 1px rgba(0, 0, 0, 0); -webkit-transform-origin: 100% 0; transform-origin: 100% 0;}.hvr-wobble-bottom:hover, .hvr-wobble-bottom:focus, .hvr-wobble-bottom:active { -webkit-animati
2022-07-01 14:30:01 UTC	202	IN	Data Raw: 2c 20 30 29 3b 0a 20 20 6f 76 65 72 66 6c 6f 77 3a 20 68 69 64 64 65 6e 3b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 69 74 69 6f 6e 2d 64 75 72 61 74 69 6f 6e 3a 20 30 2e 35 73 3b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 69 74 69 6f 6e 2d 64 75 72 61 74 69 6f 6e 3a 20 30 2e 35 73 3b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 69 74 69 6f 6e 2d 70 72 6f 70 65 72 74 79 3a 20 63 6f 6c 6f 72 2c 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3b 0a 20 20 74 72 61 6e 73 69 74 69 6f 6e 2d 70 72 6f 70 65 72 74 79 3a 20 63 6f 6c 6f 72 2c 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3b 0a 7d 0a 2e 68 76 72 2d 62 61 63 6b 2d 70 75 6c 73 65 3a 68 6f 76 65 72 2c 20 2e 68 76 72 2d 62 61 63 6b 2d 70 75 6c 73 65 3a 66 6f 63 75 73 2c 20 2e 68 76 72 2d 62 61 63 6b 2d 70 Data Ascii: , 0); overflow: hidden; -webkit-transition-duration: 0.5s; transition-duration: 0.5s; -webkit-transition-property: color, background-color; transition-property: color, background-color;}.hvr-back-pulse:hover, .hvr-back-pulse:focus, .hvr-back-p
2022-07-01 14:30:01 UTC	210	IN	Data Raw: 0a 20 20 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 20 6d 69 64 64 6c 65 3b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 70 65 72 73 70 65 63 74 69 76 65 28 31 70 78 29 20 74 72 61 6e 73 6c 61 74 65 5a 28 30 29 3b 0a 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 70 65 72 73 70 65 63 74 69 76 65 28 31 70 78 29 20 74 72 61 6e 73 6c 61 74 65 5a 28 30 29 3b 0a 20 20 62 6f 78 2d 73 68 61 64 6f 77 3a 20 30 20 30 20 31 70 78 20 72 67 62 61 28 30 2c 20 30 2c 20 30 2c 20 30 29 3b 0a 20 20 70 6f 73 69 74 69 6f 6e 3a 20 72 65 6c 61 74 69 76 65 3b 0a 20 20 7d 77 65 62 6b 69 74 2d 74 72 61 6e 73 69 74 69 6f 6e 2d 70 72 6f 70 65 72 74 79 3a 20 63 6f 6c 6f 72 3b 0a 20 20 74 72 61 6e 73 69 74 69 6f 6e 2d 70 72 6f 70 65 72 74 79 3a 20 63 6f 6c 6f 72 3b 0a Data Ascii: vertical-align: middle; -webkit-transform: perspective(1px) translateZ(0); transform: perspective(1px) t ranslateZ(0); box-shadow: 0 0 1px rgba(0, 0, 0, 0); position: relative; -webkit-transition-property: color; transition-propert y: color;
2022-07-01 14:30:01 UTC	218	IN	Data Raw: 6c 6f 72 3a 20 77 68 69 74 65 3b 0a 7d 0a 2e 68 76 72 2d 73 68 75 74 74 65 72 2d 69 6e 2d 68 6f 72 69 7a 6f 6e 74 61 6c 3a 68 6f 76 65 72 3a 62 65 66 6f 72 65 2c 20 2e 68 76 72 2d 73 68 75 74 74 65 72 2d 69 6e 2d 68 6f 72 69 7a 6f 6e 74 61 6c 3a 66 6f 63 75 73 3a 62 65 66 6f 72 65 2c 20 2e 68 76 72 2d 73 68 75 74 74 65 72 2d 69 6e 2d 68 6f 72 69 7a 6f 6e 74 61 6c 3a 61 63 74 69 76 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 7d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 73 63 61 6c 65 58 28 30 29 3b 0a 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 73 63 61 6c 65 58 28 30 29 3 b 0a 7d 0a 0a 2f 2a 20 53 68 75 74 74 65 72 20 4f 75 74 20 48 6f 72 69 7a 6f 6e 74 61 6c 20 2a 2f 0a 2e 68 76 72 2d 73 6 8 75 74 74 65 72 2d 6f 75 74 2d 68 6f 72 69 7a 6f 6e 74 61 6c 20 Data Ascii: lor: white;}.hvr-shutter-in-horizontal:hover:before, .hvr-shutter-in-horizontal:focus:before, .hvr-shutter-in-horizontal:active:before { -webkit-transform: scaleX(0); transform: scaleX(0);}/* Shutter Out Horizontal */.hvr-shutter-out-horizontal
2022-07-01 14:30:01 UTC	226	IN	Data Raw: 73 3b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 69 74 69 6f 6e 2d 70 72 6f 70 65 72 74 79 3a 20 74 6f 70 2c 20 72 69 67 68 74 2c 20 62 6f 74 74 6f 6d 2c 20 6c 65 66 74 3b 0a 20 20 74 72 61 6e 73 69 74 69 6f 6e 2d 70 72 6f 70 65 72 74 79 3a 20 74 6f 70 2c 20 72 69 67 68 74 2c 20 62 6f 74 74 6f 6d 2c 20 6c 65 66 74 3b 0a 7d 0a 2e 68 76 72 2d 6f 75 74 6c 69 6e 65 2d 6f 75 74 3a 68 6f 76 65 72 3a 62 65 66 6f 72 65 2c 20 2e 68 76 72 2d 6f 75 74 6c 69 6e 65 2d 6f 75 74 3a 66 6f 63 75 73 3a 62 65 66 6f 72 65 2c 20 2e 68 76 72 2d 6f 75 74 6c 69 6e 65 2d 6f 75 74 3a 61 63 74 69 76 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 74 6f 70 3a 20 2d 38 70 78 3b 0a 20 20 72 69 67 68 74 3a 20 2d 38 70 78 3b 0a 20 20 62 6f 74 74 6f 6d 3a 20 2d 38 70 78 3b 0a 20 20 6c 65 66 Data Ascii: s; -webkit-transition-property: top, right, bottom, left; transition-property: top, right, bottom, left;}.hvr-outline-out:hover:before, .hvr-outline-out:focus:before, .hvr-outline-out:active:before { top: -8px; right: -8px; bottom: -8px; lef
2022-07-01 14:30:01 UTC	234	IN	Data Raw: 6f 6e 3a 20 65 61 73 65 2d 6f 75 74 3b 0a 7d 0a 2e 68 76 72 2d 75 6e 64 65 72 6c 69 6e 65 2d 72 65 76 65 61 6c 3a 68 6f 76 65 72 3a 62 65 66 6f 72 65 2c 20 2e 68 76 72 2d 75 6e 64 65 72 6c 69 6e 65 2d 72 65 76 65 61 6c 3a 61 63 74 69 76 63 75 73 3a 62 65 66 6f 72 65 2c 20 2e 68 76 72 2d 75 6e 64 65 72 6c 69 6e 65 2d 72 65 76 65 61 6c 3a 61 63 74 69 76 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 59 28 30 29 3b 0a 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 59 28 30 29 3b 0a 7d 0a 0a 2f 2a 20 4f 76 65 72 6c 69 6e 65 20 52 65 76 65 61 6c 20 2a 2f 0a 2e 68 76 72 2d 6f 76 65 72 6c 69 6e 65 2d 72 65 76 65 61 6c 20 7b 0a 20 20 64 69 73 70 6c 61 79 3a 20 69 6e 6c 69 6e 65 Data Ascii: on: ease-out;}.hvr-underline-reveal:hover:before, .hvr-underline-reveal:focus:before, .hvr-underline-reveal: active:before { -webkit-transform: translateY(0); transform: translateY(0);}/* Overline Reveal */.hvr-overline-reveal { display: inline
2022-07-01 14:30:01 UTC	241	IN	Data Raw: 79 3a 20 74 72 61 6e 73 66 6f 72 6d 3b 0a 20 20 74 6f 70 3a 20 63 61 6c 63 28 35 30 25 20 2d 20 31 30 70 78 29 3b 0a 20 20 72 69 67 68 74 3a 20 30 3b 0a 20 20 62 6f 72 64 65 72 2d 77 69 64 74 68 3a 20 31 30 70 78 20 30 20 31 30 70 78 20 31 30 70 78 3b 0a 20 20 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 20 74 72 61 6e 73 70 61 72 65 6e 74 20 74 72 61 6e 73 70 61 72 65 6e 74 20 74 72 61 6e 73 70 61 72 65 6e 74 20 23 65 31 65 31 65 31 3b 0a 7d 0a 2e 68 76 72 2d 62 75 62 62 6c 65 2d 72 69 67 68 74 3a 68 6f 76 65 72 3a 62 65 66 6f 72 65 2c 20 2e 68 76 72 2d 62 75 62 62 6c 65 2d 72 6 9 67 68 74 3a 66 6f 63 75 73 3a 62 65 66 6f 72 65 2c 20 2e 68 76 72 2d 62 75 62 62 6c 65 2d 72 69 67 68 74 3a 61 63 74 69 76 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 2d 77 65 62 6b 69 74 Data Ascii: y: transform; top: calc(50% - 10px); right: 0; border-width: 10px 0 10px 10px; border-color: transparent transparent transparent #e1e1e1;}.hvr-bubble-right:hover:before, .hvr-bubble-right:focus:before, .hvr-bubble-right:acti ve:before { -webkit
2022-07-01 14:30:01 UTC	249	IN	Data Raw: 68 76 72 2d 69 63 6f 6e 2d 66 6f 72 77 61 72 64 3a 66 6f 63 75 73 20 2e 68 76 72 2d 69 63 6f 6e 2c 20 2e 68 76 72 2d 69 63 6f 6e 2d 66 6f 72 77 61 72 64 3a 61 63 74 69 76 65 20 2e 68 76 72 2d 69 63 6f 6e 20 7b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 58 28 34 70 78 29 3b 0a 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 58 28 34 70 78 29 3b 0a 7d 0a 0a 2f 2a 20 49 63 6f 6e 20 44 6f 77 6e 20 2a 2f 0a 40 2d 77 65 62 6b 69 74 2d 6b 65 79 66 72 61 6d 65 73 20 68 76 72 2d 69 63 6f 6e 2d 64 6f 77 6e 20 7b 0a 2 0 20 30 25 2c 0a 09 35 30 25 2c 0a 09 31 30 30 25 20 7b 0a 20 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 59 28 30 29 3b 0a 20 20 20 20 Data Ascii: hvr-icon-forward:focus .hvr-icon, .hvr-icon-forward:active .hvr-icon { -webkit-transform: translateX(4px); transform: translateX(4px);}/* Icon Down */@-webkit-keyframes hvr-icon-down { 0%,50%,100% { -webkit-transform: translateY(0);

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	383	IN	Data Raw: 6f 6e 2d 73 68 72 69 6e 6b 20 7b 0a 20 20 64 69 73 70 6c 61 79 3a 20 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 0a 20 20 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 20 6d 69 64 64 6c 65 3b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 70 65 72 73 70 65 63 74 69 76 65 28 31 70 78 29 20 74 72 61 6e 73 6c 61 74 65 5a 28 30 29 3b 0a 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 70 65 72 73 70 65 63 74 69 76 65 28 31 70 78 29 20 74 72 61 6e 73 6c 61 74 65 5a 28 30 29 3b 0a 20 20 62 6f 78 2d 73 68 61 64 6f 77 3a 20 30 20 30 20 31 70 78 20 72 67 62 61 28 30 2c 20 30 2c 20 30 29 3b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 69 74 69 6f 6e 2d 64 75 72 61 74 69 6f 6e 3a 20 30 2e 33 73 3b 0a 20 20 74 72 61 6e 73 69 74 69 6f 6e 2d 64 75 72 61 Data Ascii: on-shrink { display: inline-block; vertical-align: middle; -webkit-transform: perspective(1px) translateZ(0); transform: perspective(1px) translateZ(0); box-shadow: 0 0 1px rgba(0, 0, 0, 0); -webkit-transition-duration: 0.3s; transition-duration: 0.3s;}
2022-07-01 14:30:01 UTC	391	IN	Data Raw: 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 5a 28 30 29 3b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 69 74 69 6f 6e 2d 64 75 72 61 74 69 6f 6e 3a 20 30 2e 33 73 3b 0a 20 20 74 72 61 6e 73 69 74 69 6f 6e 2d 70 72 6f 70 65 72 74 79 3a 20 74 72 61 6e 73 66 6f 72 6d 3b 0a 20 20 74 72 61 6e 73 69 74 69 6f 6e 2d 70 72 6f 70 65 72 74 79 3a 20 74 72 61 6e 73 66 6f 72 6d 3b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 69 74 69 6f 6e 2d 74 69 6d 69 6e 67 2d 66 75 6e 63 74 69 6f 6e 3a 20 65 61 73 65 2d 6f 75 74 3b 0a 20 20 74 72 61 6e 73 69 74 69 6f 6e 2d 74 69 6d 69 6e 67 2d 66 75 6e 63 74 69 6f 6e 3a 20 65 61 73 65 2d 6f 75 74 3b Data Ascii: transform: translateZ(0); -webkit-transition-duration: 0.3s; transition-duration: 0.3s; -webkit-transition-property: transform; transition-property: transform; -webkit-transition-timing-function: ease-out; transition-timing-function: ease-out;
2022-07-01 14:30:01 UTC	399	IN	Data Raw: 73 70 65 63 74 69 76 65 28 31 70 78 29 20 74 72 61 6e 73 6c 61 74 65 5a 28 30 29 3b 0a 20 20 62 6f 78 2d 73 68 61 64 6f 77 3a 20 30 20 30 20 31 70 78 20 72 67 62 61 28 30 2c 20 30 2c 20 30 2c 20 30 29 3b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 69 74 69 6f 6e 2d 64 75 72 61 74 69 6f 6e 3a 20 30 2e 33 73 3b 0a 20 20 74 72 61 6e 73 69 74 69 6f 6e 2d 64 75 72 61 74 69 6f 6e 3a 20 30 2e 33 73 3b 0a 7d 0a 2e 68 76 72 2d 69 63 6f 6e 2d 77 6f 62 62 6c 65 2d 68 6f 72 69 7a 6f 6e 74 61 6c 20 2e 68 76 72 2d 69 63 6f 6e 20 7b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 5a 28 30 29 3b 0a 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 5a 28 30 29 3b 0a 7d 0a 2e 68 76 72 2d 69 63 6f 6e 2d 77 6f Data Ascii: spectvie(1px) translateZ(0); box-shadow: 0 0 1px rgba(0, 0, 0, 0); -webkit-transition-duration: 0.3s; transition-duration: 0.3s;}.hvr-icon-wobble-horizontal .hvr-icon { -webkit-transform: translateZ(0); transform: translateZ(0);}.hvr-icon-wo
2022-07-01 14:30:01 UTC	407	IN	Data Raw: 6f 72 65 2c 20 2e 68 76 72 2d 63 75 72 6c 2d 74 6f 70 2d 6c 65 66 74 3a 66 6f 63 75 73 3a 62 65 66 6f 72 65 2c 20 2e 68 76 72 2d 63 75 72 6c 2d 74 6f 70 2d 6c 65 66 74 3a 61 63 74 69 76 65 3a 62 65 66 6f 72 65 20 7b 0a 20 20 77 69 64 74 68 3a 20 32 35 70 78 3b 0a 20 20 68 65 69 67 68 74 3a 20 32 35 70 78 3b 0a 7d 0a 0a 2f 2a 20 43 75 72 6c 20 54 6f 70 20 52 69 67 68 74 20 2a 2f 0a 2e 68 76 72 2d 63 75 72 6c 2d 74 6f 70 2d 72 69 67 68 74 20 7b 0a 20 20 64 69 73 70 6c 61 79 3a 20 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 0a 20 20 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 20 6d 69 64 64 6c 65 3b 0a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 70 65 72 73 70 65 63 74 69 76 65 28 31 70 78 29 20 74 72 61 6e 73 6c 61 74 65 5a 28 30 29 3b 0a 20 Data Ascii: ore, .hvr-curl-top-left:focus:before, .hvr-curl-top-left:active:before { width: 25px; height: 25px;}/* Curl Top Right */.hvr-curl-top-right { display: inline-block; vertical-align: middle; -webkit-transform: perspective(1px) translateZ(0);

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49817	104.18.10.207	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	27	OUT	GET /bootstrap/4.0.0/css/bootstrap.min.css HTTP/1.1 Host: maxcdn.bootstrapcdn.com Connection: keep-alive Origin: https://eyecandylashcompany.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: text/css,*/*;q=0.1 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: style Referer: https://eyecandylashcompany.com/payment/frontend_paper_lantern/index.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	27	IN	HTTP/1.1 200 OK Date: Fri, 01 Jul 2022 14:30:01 GMT Content-Type: text/css; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding CDN-PullZone: 252412 CDN-Uid: b1941f61-b576-4f40-80de-5677acb38f74 CDN-RequestCountryCode: DE Access-Control-Allow-Origin: * Cache-Control: public, max-age=31919000 Last-Modified: Mon, 25 Jan 2021 22:04:04 GMT CDN-CachedAt: 06/09/2022 14:01:47 CDN-EdgeStorageId: 756 CDN-RequestPullCode: 200 CDN-RequestPullSuccess: True timing-allow-origin: * cross-origin-resource-policy: cross-origin X-Content-Type-Options: nosniff CDN-Status: 200 CDN-ProxyVer: 1.02 CDN-RequestId: 7e1906d1cdbefbd57a6262b1abd6a503 CDN-Cache: HIT CF-Cache-Status: HIT Age: 72501 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Server: cloudflare CF-RAY: 723fd65108fd918e-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-01 14:30:01 UTC	28	IN	Data Raw: 37 62 65 63 0d 0a 2f 2a 21 0a 20 2a 20 42 6f 6f 74 73 74 72 61 70 20 76 34 2e 30 2e 30 20 28 68 74 74 70 73 3a 2f 2f 67 65 74 62 6f 6f 74 73 74 72 61 70 2e 63 6f 6d 29 0a 20 2a 20 43 6f 70 79 72 69 67 68 74 20 32 30 31 31 2d 32 30 31 38 20 54 68 65 20 42 6f 6f 74 73 74 72 61 70 20 41 75 74 68 6f 72 73 0a 20 2a 20 43 6f 70 79 72 69 67 68 74 20 32 30 31 31 2d 32 30 31 38 20 54 77 69 74 74 65 72 2c 20 49 6e 63 2e 0a 20 2a 20 4c 69 63 65 6e 73 65 64 20 75 6e 64 65 72 20 4d 49 54 20 28 68 74 74 70 73 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 74 77 62 73 2f 62 6f 6f 74 73 74 72 61 70 2f 62 6c 6f 62 2f 6d 61 73 74 65 72 2f 4c 49 43 45 4e 53 45 29 0a 20 2a 2f 3a 72 6f 6f 74 7b 2d 2d 62 6c 75 65 3a 23 30 30 37 62 66 66 3b 2d 2d 69 6e 64 69 67 6f 6f 3a 23 36 36 31 30 Data Ascii: 7bec/*! * Bootstrap v4.0.0 (https://getbootstrap.com) * Copyright 2011-2018 The Bootstrap Authors * Copyright 2011-2018 Twitter, Inc. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE) */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e91e63;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;--green:#28a745;--teal:#20a997;--blue-gray:#17a2b8;--light:#f8d7da;--light-gray:#d6d8db;--dark:#343a40;--dark-gray:#6c757d;--white:#fff}
2022-07-01 14:30:01 UTC	29	IN	Data Raw: 6c 3a 23 32 30 63 39 39 37 3b 2d 2d 63 79 61 6e 3a 23 31 37 61 32 62 38 3b 2d 2d 77 68 69 74 65 3a 23 66 66 66 3b 2d 2d 67 72 61 79 3a 23 36 63 37 35 37 64 3b 2d 2d 67 72 61 79 2d 64 61 72 6b 3a 23 33 34 33 61 34 30 3b 2d 2d 70 72 69 6d 61 72 79 3a 23 30 30 37 62 66 66 3b 2d 2d 73 65 63 6f 6e 64 61 72 79 3a 23 36 63 37 35 37 64 3b 2d 2d 73 75 63 63 65 73 73 3a 23 32 38 61 37 34 35 3b 2d 2d 69 6e 66 6f 3a 23 31 37 61 32 62 38 3b 2d 2d 77 61 72 6e 69 6e 67 3a 23 66 66 63 31 30 37 3b 2d 2d 64 61 6e 67 65 72 3a 23 64 63 33 35 34 35 3b 2d 2d 6c 69 67 68 74 3a 23 66 38 66 39 66 61 3b 2d 2d 64 61 72 6b 3a 23 33 34 33 61 34 30 3b 2d 2d 62 72 65 61 6b 70 6f 69 6e 74 2d 78 73 3a 30 3b 2d 2d 62 72 65 61 6b 70 6f 69 6e 74 2d 78 73 3a 30 3b 2d 2d 62 72 65 61 6b 70 6f 69 6e 74 2d 73 6d 3a 35 37 36 70 78 3b 2d 2d 62 72 65 Data Ascii: l:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8d7da;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--bre
2022-07-01 14:30:01 UTC	30	IN	Data Raw: 64 61 74 61 2d 6f 72 69 67 69 6e 61 6c 2d 74 69 74 6c 65 5d 2c 61 62 62 72 5b 74 69 74 6c 65 5d 7b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 75 6e 64 65 72 6c 69 6e 65 3b 2d 77 65 62 6b 69 74 2d 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 75 6e 64 65 72 6c 69 6e 65 20 64 6f 74 74 65 64 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 75 6e 64 65 72 6c 69 6e 65 20 64 6f 74 74 65 64 3b 63 75 72 73 6f 72 3a 68 65 6c 70 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 30 7d 61 64 64 72 65 73 73 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 6e 6f 72 6d 61 6c 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 69 6e 68 65 72 69 74 7d 64 6c 2c 6f 6c 2c 75 6c 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 72 67 69 6e 2d Data Ascii: data-original-title},abbr[title]{text-decoration:underline;webkit-text-decoration:underline dotted;text-decoration:underline dotted;cursor:help;border-bottom:0}address{margin-bottom:1rem;font-style:normal;line-height:inherit}dl,ol,ul{margin-top:0;margin-
2022-07-01 14:30:01 UTC	31	IN	Data Raw: 74 6f 6d 3a 2e 35 72 65 6d 7d 62 75 74 74 6f 6e 7b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 30 7d 62 75 74 74 6f 6e 3a 66 6f 63 73 7b 6f 75 74 6c 69 6e 65 3a 31 70 78 20 64 6f 74 74 65 64 3b 6f 75 74 6c 69 6e 65 3a 35 70 78 20 61 75 74 6f 20 2d 77 65 62 6b 69 74 2d 66 6f 63 75 73 2d 72 69 6e 67 2d 63 6f 6c 6f 72 7d 62 75 74 74 6f 6e 2c 69 6e 70 75 74 2c 6f 70 74 67 72 6f 75 70 2c 73 65 6c 65 63 74 2c 74 65 78 74 61 72 65 61 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 69 6e 68 65 72 69 74 3b 66 6f 6e 74 2d 73 69 7a 65 3a 69 6e 68 65 72 69 74 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 69 6e 68 65 72 69 74 7d 62 75 74 74 6f 6e 2c 69 6e 70 75 74 7b 6f 76 65 72 66 6c 6f 77 3a 76 69 73 69 62 6c 65 7d 62 75 74 74 6f 6e 2c 73 65 6c 65 63 74 Data Ascii: tom;.5rem)button{border-radius:0}button:focus{outline:1px dotted;outline:5px auto -webkit-focus-ring-color}button,input,optgroup,select,textarea{margin:0;font-family:inherit;font-size:inherit;line-height:inherit}button,input{overflow:visible}button,select
2022-07-01 14:30:01 UTC	33	IN	Data Raw: 68 69 64 64 65 6e 5d 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 68 31 2c 2e 68 32 2c 2e 68 33 2c 2e 68 34 2c 2e 68 35 2c 2e 68 36 2c 68 31 2c 68 32 2c 68 33 2c 68 34 2c 68 35 2c 68 36 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 2e 35 72 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 69 6e 68 65 72 69 74 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 35 30 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 2e 32 3b 63 6f 6c 6f 72 3a 69 6e 68 65 72 69 74 7d 2e 68 31 2c 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 35 72 65 6d 7d 2e 68 32 2c 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 72 65 6d 7d 2e 68 33 2c 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 35 72 65 6d 7d 2e 68 34 2c 68 34 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 7d 2e Data Ascii: hidden}[display:none!important].h1,.h2,.h3,.h4,.h5,.h6,h1,h2,h3,h4,h5,h6{margin-bottom:.5rem;font-family:inherit;font-weight:500;line-height:1.2;color:inherit}.h1,h1{font-size:2.5rem}.h2,h2{font-size:2rem}.h3,h3{font-size:1.75rem}.h4,h4{font-size:1.5rem}.

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	45	IN	Data Raw: 6c 65 78 3a 30 3b 2d 6d 73 2d 66 6c 65 78 3a 30 20 30 20 39 31 2e 36 36 36 36 36 37 25 3b 66 6c 65 78 3a 30 20 30 20 39 31 2e 36 36 36 36 36 37 25 3b 6d 61 78 2d 77 69 64 74 68 3a 39 31 2e 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 6c 67 2d 31 32 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 66 6c 65 78 3a 30 3b 2d 6d 73 2d 66 6c 65 78 3a 30 20 30 2 0 31 30 30 25 3b 66 6c 65 78 3a 30 20 30 20 31 30 30 25 3b 6d 61 78 2d 77 69 64 74 68 3a 31 30 30 25 7d 2e 6f 72 64 65 72 2d 6c 67 2d 66 69 72 73 74 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 30 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 72 3a 2d 31 3b 6f 72 64 65 72 3a 2d 31 7d 2e 6f 72 64 65 72 2d 6c 67 2d 6c 61 73 74 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 Data Ascii: lex:0;-ms-flex:0 0 91.666667%;flex:0 0 91.666667%;max-width:91.666667%;col-lg-12{-webkit-box-flex:0;-ms-flex:0 0 100%;flex:0 0 100%;max-width:100%;order-lg-first{-webkit-box-ordinal-group:0;-ms-flex-order:-1;order:-1}.order-lg-last{-webkit-box-ordinal-g
2022-07-01 14:30:01 UTC	46	IN	Data Raw: 66 74 3a 35 30 25 7d 2e 6f 66 66 73 65 74 2d 6c 67 2d 37 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 35 38 2e 33 33 33 33 33 25 7d 2e 6f 66 66 73 65 74 2d 6c 67 2d 38 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 36 36 2e 36 36 36 36 37 25 7d 2e 6f 66 66 73 65 74 2d 6c 67 2d 31 30 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 38 33 2e 33 33 33 33 33 25 7d 2e 6f 66 66 73 65 74 2d 6 c 67 2d 31 31 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 39 31 2e 36 36 36 36 36 37 25 7d 7d 40 6d 65 64 69 61 20 28 6d 69 6e 2d 77 69 64 74 68 3a 31 32 30 30 70 78 29 7b 2e 63 6f 6c 2d 78 6c 7b 2d 6d 73 2d 66 6c 65 78 2d 70 72 65 66 65 72 72 65 64 2d 73 69 7a 65 3a 30 3b 66 6c 65 78 2d 62 61 73 69 73 3a 30 Data Ascii: ft:50%).offset-lg-7{margin-left:58.333333%}.offset-lg-8{margin-left:66.666667%}.offset-lg-9{margin-left:75%}.offset-lg-10{margin-left:83.333333%}.offset-lg-11{margin-left:91.666667%}}@media (min-width:1200px){.col-xl{-ms-flex-pr eferred-size:0;flex-basis:0
2022-07-01 14:30:01 UTC	47	IN	Data Raw: 68 3a 39 31 2e 36 36 36 36 36 37 25 7d 2e 63 6f 6c 2d 78 6c 2d 31 32 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 66 6c 65 78 3a 30 3b 2d 6d 73 2d 66 6c 65 78 3a 30 20 30 20 31 30 30 25 3b 6d 61 78 2d 77 69 64 74 68 3a 31 30 30 25 7d 2e 6f 72 64 65 72 2d 78 6c 2d 66 69 72 73 74 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 69 6e 61 6c 2d 67 72 6f 75 70 3a 30 3b 2d 6d 73 2d 66 6c 65 78 2d 6f 72 64 65 72 3a 2d 31 3b 6f 72 64 65 72 3a 2d 31 7d 2e 6f 72 64 65 72 2d 78 6c 2d 6c 61 73 74 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 64 65 72 3a 31 33 3b 6f 72 64 65 72 3a 31 33 7d 2e 6f 72 64 65 72 2d 78 6c 2d 30 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 Data Ascii: h:91.666667%;col-xl-12{-webkit-box-flex:0;-ms-flex:0 0 100%;flex:0 0 100%;max-width:100%;order-xl-first{-w ebkit-box-ordinal-group:0;-ms-flex-order:-1;order:-1}.order-xl-last{-webkit-box-ordinal-group:14;-ms-flex-order:13;order :13}.order-xl-0{-webkit-box
2022-07-01 14:30:01 UTC	49	IN	Data Raw: 72 67 69 6e 2d 6c 65 66 74 3a 36 36 2e 36 36 36 36 36 37 25 7d 2e 6f 66 66 73 65 74 2d 78 6c 2d 39 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 37 35 25 7d 2e 6f 66 66 73 65 74 2d 78 6c 2d 31 30 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 38 33 2e 33 33 33 33 33 25 7d 2e 6f 66 66 73 65 74 2d 78 6c 2d 31 31 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 39 31 2e 36 36 36 36 36 37 25 7d 7d 2e 74 61 62 6c 65 7b 77 69 64 74 68 3a 31 30 30 25 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 74 72 61 6e 73 70 61 72 65 6e 74 7d 2e 74 61 62 6c 65 20 74 64 2c 2e 74 61 62 6c 65 20 74 68 7b 70 61 64 64 69 6e 67 3a 2e 37 35 72 65 6d 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e Data Ascii: rgin-left:66.666667%).offset-xl-9{margin-left:75%}.offset-xl-10{margin-left:83.333333%}.offset-xl-11{margin-left:91.666667%}}.table{width:100%;max-width:100%;margin-bottom:1rem;background-color:transparent}.table td,.table th{padding:.75rem;vertical-align
2022-07-01 14:30:01 UTC	50	IN	Data Raw: 62 6c 65 2d 73 75 63 63 65 73 73 3a 68 6f 76 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 62 31 64 66 62 62 7d 2e 74 61 62 6c 65 2d 68 6f 76 65 72 20 2e 74 61 62 6c 65 2d 73 75 63 63 65 73 73 3a 68 6f 76 65 72 3e 74 64 2c 2e 74 61 62 6c 65 2d 68 6f 76 65 72 20 2e 74 61 62 6c 65 2d 73 75 63 63 65 73 73 3a 68 6f 76 65 72 3e 74 68 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 62 31 64 66 62 62 7d 2e 74 61 62 6c 65 2d 69 6e 66 6f 2c 2e 74 61 62 6c 65 2d 69 6e 66 6f 3e 74 64 2c 2e 74 61 62 6c 65 2d 69 6e 66 6f 3e 74 68 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 62 65 65 35 65 62 7d 2e 74 61 62 6c 65 2d 68 6f 76 65 72 20 2e 74 61 62 6c 65 2d 69 6e 66 6f 3a 68 6f 76 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f Data Ascii: ble-success: hover{background-color:#b1dffb}.table-hover .table-success: hover>td,.table-hover .table-success: hover>th{background-color:#b1dffb}.table-info,.table-info>td,.table-info>th{background-color:#bee5eb}.table-hover .table-info: hover{background-colo
2022-07-01 14:30:01 UTC	51	IN	Data Raw: 76 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 72 67 62 61 28 30 2c 30 2c 30 2c 2e 30 37 35 29 7d 2e 74 61 62 6c 65 2d 68 6f 76 65 72 20 2e 74 61 62 6c 65 2d 61 63 74 69 76 65 3a 68 6f 76 65 72 3e 74 64 2c 2e 74 61 62 6c 65 2d 68 6f 76 65 72 20 2e 74 61 62 6c 65 2d 61 63 74 69 76 65 3a 68 6f 76 65 72 3e 74 68 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 72 67 62 61 28 30 2c 30 2c 30 2c 2e 30 37 35 29 7d 2e 74 61 62 6c 65 20 2e 74 68 65 61 64 2d 64 61 72 6b 20 74 68 7b 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 32 31 32 35 32 39 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 33 32 33 38 33 65 7d 2e 74 61 62 6c 65 20 2e 74 68 6 5 61 64 2d 6c 69 67 68 74 20 74 68 7b 63 6f 6c 6f 72 3a 23 34 39 Data Ascii: ver{background-color:rgba(0,0,0,.075)}.table-hover .table-active: hover>td,.table-hover .table-active: hover>th{background-color:rgba(0,0,0,.075)}.table .thead-dark th{color:#fff;background-color:#212529;border-color:#32383e}.table .thead-light th{color:#49
2022-07-01 14:30:01 UTC	53	IN	Data Raw: 6b 69 74 2d 6f 76 65 72 66 6c 6f 77 2d 73 63 72 6f 6c 6c 69 6e 67 3a 74 6f 75 63 68 3b 2d 6d 73 2d 6f 76 65 72 66 6c 6f 77 2d 73 74 79 6c 65 3a 2d 6d 73 2d 61 75 74 6f 68 69 64 69 6e 67 2d 73 63 72 6f 6c 6c 62 61 72 7d 2e 74 61 62 6c 65 2d 72 65 73 70 6f 6e 73 69 76 65 2d 78 6c 3e 2e 74 61 62 6c 65 2d 62 6f 72 64 65 72 65 64 7b 62 6f 72 64 65 72 3a 30 7d 7d 2e 74 61 62 6c 65 2d 72 65 73 70 6f 6e 73 69 76 65 7b 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 6f 76 65 72 66 6c 6f 77 2d 78 3a 61 75 74 6f 3b 2d 77 65 62 6b 69 74 2d 6f 76 65 72 66 6c 6f 77 2d 73 63 72 6f 6c 6c 69 6e 67 3a 74 6f 75 63 68 3b 2d 6d 73 2d 6f 76 65 72 66 6c 6f 77 2d 73 74 79 6c 65 3a 2d 6d 73 2d 61 75 74 6f 68 69 64 69 6e 67 2d 73 63 72 6f 6c 6c 62 61 72 Data Ascii: kit-overflow-scrolling:touch;-ms-overflow-style:-ms-autohiding-scrollbar}.table-responsive-xl>.table-bordere d{border:0}.table-responsive{display:block;width:100%;overflow-x:auto;-webkit-overflow-scrolling:touch;-ms-overflow-sty le:-ms-autohiding-scrollbar
2022-07-01 14:30:01 UTC	54	IN	Data Raw: 61 64 64 69 6e 67 2d 74 6f 70 3a 63 61 6c 63 28 2e 33 37 35 72 65 6d 20 2b 20 31 70 78 29 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 63 61 6c 63 28 2e 33 37 35 72 65 6d 20 2b 20 31 70 78 29 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 69 6e 68 65 72 69 74 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 2 e 35 7d 2e 63 6f 6c 2d 66 6f 72 6d 6c 61 62 65 6c 2d 6c 67 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 63 61 6c 63 28 2e 35 72 65 6d 20 2b 20 31 70 78 29 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 63 61 6c 63 28 2e 35 72 65 6d 20 2b 20 31 70 78 29 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 35 72 65 6d 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 2e 35 7d 2e 63 6f 6c 2d 66 6f 72 6d 2d 6c 61 62 65 6c 2d 73 6d 7b 70 61 64 64 Data Ascii: adding-top:calc(.375rem + 1px);padding-bottom:calc(.375rem + 1px);margin-bottom:0;font-size:inherit;line-hei ght:1.5}.col-form-label-lg{padding-top:calc(.5rem + 1px);padding-bottom:calc(.5rem + 1px);font-size:1.25rem;line-height: 1.5}.col-form-label-sm{padd

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	55	IN	Data Raw: 6d 2d 63 6f 6e 74 72 6f 6c 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 73 6d 3e 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 61 70 70 65 6e 64 3e 2e 62 74 6e 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 73 6d 3e 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 61 70 70 65 6e 64 3e 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 74 65 78 74 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 73 6d 3e 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 73 6d 3e 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 70 72 65 70 65 6e 64 3e 2e 62 74 6e 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 73 6d 3e 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 70 72 65 70 65 6e 64 3e 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 74 65 78 74 7b 70 61 64 64 69 6e 67 3a 2e 32 35 72 65 6d 20 2e 35 72 65 6d 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 38 37 35 72 65 6d 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 2e Data Ascii: m-control>.input-group-sm>.input-group-append>.btn,.input-group-sm>.input-group-append>.input-group-text,.input-group-sm>.input-group-prepend>.btn,.input-group-sm>.input-group-prepend>.input-group-text{padding:.25rem .5rem;font-size:.875rem;line-height:1.
2022-07-01 14:30:01 UTC	57	IN	Data Raw: 65 5d 29 3a 6e 6f 74 28 5b 6d 75 6c 74 69 70 6c 65 5d 29 2c 2e 69 6e 70 75 74 2d 67 72 6f 75 70 2d 6c 67 3e 73 65 6c 65 63 74 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 3a 6e 6f 74 28 5b 73 69 7a 65 5d 29 3a 6e 6f 74 28 5b 6d 75 6c 74 69 70 6c 65 5d 29 2c 73 65 6c 65 63 74 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 2d 6c 6f 3a 6e 6f 74 28 5b 73 69 7a 65 5d 29 3a 6e 6f 74 28 5b 6d 75 6c 74 69 70 6c 65 5d 29 7b 68 65 69 67 68 74 3a 63 61 6c 63 28 32 2e 38 37 35 72 65 6d 20 2b 20 32 70 78 29 7d 2e 66 6f 72 6d 2d 67 72 6f 75 70 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 7d 2e 66 6f 72 6d 2d 74 65 78 74 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 2e 32 35 72 65 6d 7d 2e 66 6f 72 6d 2d 72 6f 77 7b 64 69 73 70 6c 61 79 3a Data Ascii: e):not([multiple]),.input-group-lg>select.form-control:not([size]):not([multiple]),select.form-control-lg:not([size]):not([multiple]){height:calc(2.875rem + 2px));.form-group{margin-bottom:1rem}.form-text{display:block;margin-top:.25rem}.form-row{display:
2022-07-01 14:30:01 UTC	58	IN	Data Raw: 6d 2d 63 6f 6e 74 72 6f 6c 3a 76 61 6c 69 64 7b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 63 2a 23 32 38 61 37 34 35 7d 2e 63 75 73 74 6f 6d 2d 73 65 6c 65 63 74 2e 69 73 2d 76 61 6c 69 64 3a 66 6f 63 75 73 2c 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 2e 69 73 2d 76 61 6c 69 64 3a 66 6f 63 75 73 2c 2e 77 61 73 2d 76 61 6c 69 64 61 74 65 64 20 2e 63 75 73 74 6f 6d 2d 73 65 6c 65 63 74 3a 76 61 6c 69 64 3a 66 6f 63 75 73 2c 2e 77 61 73 2d 76 61 6c 69 64 61 74 65 64 20 2e 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 3a 76 61 6c 69 64 3a 66 6f 63 75 73 7b 62 6f 72 6d 63 6f 6c 6f 72 3a 63 61 37 34 35 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 30 20 20 2e 32 72 65 6d 20 72 67 62 61 28 34 30 2c 31 36 3 7 2c 36 39 2c 2e 32 35 29 7d 2e 63 75 73 74 6f 6d 2d 73 65 6c 65 Data Ascii: m-control:valid{border-color:#28a745}.custom-select.is-valid:focus,.form-control.is-valid:focus,.was-validated .custom-select:valid:focus,.was-validated .form-control:valid:focus{border-color:#28a745;box-shadow:0 0 0 .2rem rgba(40,167,69,.25)}.custom-sele
2022-07-01 14:30:01 UTC	59	IN	Data Raw: 38 30 30 30 0d 0a 2e 69 73 2d 76 61 6c 69 64 7e 2e 76 61 6c 69 64 2d 66 65 65 64 62 61 63 6b 2c 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 2d 69 6e 70 75 74 2e 69 73 2d 76 61 6c 69 64 7e 2e 76 61 6c 69 64 2d 74 6f 6f 6c 74 69 70 2c 2e 77 61 73 2d 76 61 6c 69 64 61 74 65 64 20 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 2d 69 6e 70 75 74 3a 76 61 6c 69 64 7e 2e 76 61 6c 69 64 2d 66 65 65 64 62 61 63 6b 2c 2e 77 61 73 2d 76 61 6c 69 64 61 74 65 64 20 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 2d 69 6e 70 75 74 3a 76 61 6c 69 64 7e 2e 76 61 6c 69 64 2d 74 6f 6f 6c 74 69 70 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 7d 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 2d 69 6e 70 75 74 2e 69 73 2d 76 61 6c 69 64 3a 63 68 65 63 6b 65 64 7e 2e 63 75 73 74 6f 6d Data Ascii: 8000.is-valid~.valid-feedback,.custom-control-input.is-valid~.valid-tooltip,.was-validated .custom-control-input:valid~.valid-feedback,.was-validated .custom-control-input:valid~.valid-tooltip{display:block}.custom-control-input.is-valid:checked~.custom
2022-07-01 14:30:01 UTC	61	IN	Data Raw: 78 3a 35 3b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 3b 6d 61 78 2d 77 69 64 74 68 3a 31 30 30 25 3b 70 61 64 64 69 6e 67 3a 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 2e 31 72 65 6d 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 38 37 35 72 65 6d 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 3b 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 72 67 62 61 28 32 32 30 2c 35 33 2c 36 39 2c 2e 38 29 3b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 2e 32 72 65 6d 7d 2e 63 75 73 74 6f 6d 2d 73 65 6c 65 63 74 2e 69 73 2d 69 6e 76 61 6c 69 64 2c 2e 66 6f 72 6d 2 d 63 6f 6e 74 72 6f 6c 2e 69 73 2d 69 6e 76 61 6c 69 64 2c 2e 77 61 73 2d 76 61 6c 69 64 61 74 65 64 20 2e 63 75 73 74 6f 6d 2d 73 65 6c 65 63 74 3a 69 6e 76 61 6c 69 64 2c 2e 77 61 73 Data Ascii: x:5;display:none;max-width:100%;padding:.5rem;margin-top:1rem;font-size:.875rem;line-height:1;color:#fff;background-color:rgba(220,53,69,.8);border-radius:.2rem}.custom-select.is-invalid,.form-control.is-invalid,.was-validated .custom-select:invalid,.was
2022-07-01 14:30:01 UTC	62	IN	Data Raw: 6c 69 64 7e 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 2d 6c 61 62 65 6c 7b 63 6f 6c 6f 72 3a 23 64 63 33 35 34 35 7d 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 2d 69 6e 70 75 74 2e 69 73 2d 69 6e 76 61 6c 69 64 7e 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 2d 6c 61 62 65 6c 3a 3a 62 65 66 6f 72 65 2c 2e 77 61 73 2d 76 61 6c 69 64 61 74 65 64 20 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 2d 69 6e 70 75 74 3a 69 6e 76 61 6c 69 64 7e 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 2d 6c 61 62 65 6c 3a 3a 62 65 66 6f 72 65 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 65 66 61 32 61 39 7d 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 2d 69 6e 70 75 74 2e 69 73 2d 69 6e 76 61 6c 69 64 7e 2e 69 6e 76 61 6c 69 64 2d 66 65 65 64 62 61 63 6b 2c 2e Data Ascii: lid~.custom-control-label{color:#dc3545}.custom-control-input.is-invalid~.custom-control-label::before,.was-validated .custom-control-input:invalid~.custom-control-label::before{background-color:#efa2a9}.custom-control-input.is-invalid~.invalid-feedback,.
2022-07-01 14:30:01 UTC	63	IN	Data Raw: 75 73 7e 2e 63 75 73 74 6f 6d 2d 66 69 6c 65 2d 6c 61 62 65 6c 2c 2e 77 61 73 2d 76 61 6c 69 64 61 74 65 64 20 2e 63 75 73 74 6f 6d 2d 66 69 6c 65 2d 69 6e 70 75 74 3a 69 6e 76 61 6c 69 64 3a 66 6f 63 75 73 7e 2e 63 75 73 74 6f 6d 2d 66 69 6c 65 2d 6c 61 62 65 6c 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 30 20 20 2e 32 72 65 6d 20 72 67 62 61 28 32 32 30 2c 35 33 2c 36 39 2c 2e 32 35 29 7d 2e 66 6f 72 6d 2d 69 6e 6c 69 6e 65 7b 64 69 73 70 6c 61 79 3a 2d 77 65 62 6b 69 74 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 2d 6d 73 2d 66 6c 65 78 62 6f 78 3b 64 69 73 70 6c 61 79 3a 6 6 6c 65 78 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 69 65 6e 74 3a 68 6f 72 69 7a 6f 6e 74 61 6c 3b 2d 77 65 62 6b 6 9 74 2d 62 6f 78 2d 64 69 72 65 63 74 69 6f 6e 3a 6e 6f 72 6d 61 Data Ascii: us~.custom-file-label,.was-validated .custom-file-input:invalid:focus~.custom-file-label{box-shadow:0 0 0 .2rem rgba(220,53,69,.25)}.form-inline{display:-webkit-box;display:-ms-flexbox;display:flex;-webkit-box-orient:horizontal;-webkit-box-direction:norma
2022-07-01 14:30:01 UTC	65	IN	Data Raw: 66 74 3a 30 7d 2e 66 6f 72 6d 2d 69 6e 6c 69 6e 65 20 2e 66 6f 72 6d 2d 63 68 65 63 6b 2d 69 6e 70 75 74 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 2e 32 35 72 65 6d 3b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 30 7d 2e 66 6f 72 6d 2d 69 6e 6c 69 6e 65 20 2e 63 75 73 74 6f 6d 2d 63 6f 6e 74 72 6f 6c 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 2d 6d 73 2d 66 6c 65 78 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 70 61 63 6b 3a 63 65 6e 74 65 72 3b 2d 6d 73 2d 66 6c 65 78 2d 70 61 63 6b 3a 63 65 6e 74 65 72 3b 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e Data Ascii: ft:0}.form-inline .form-check-input{position:relative;margin-top:0;margin-right:.25rem;margin-left:0}.form-inline .custom-control{-webkit-box-align:center;-ms-flex-align:center;align-items:center;-webkit-box-pack:center;-ms-flex-pack:center;justify-conten

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	66	IN	Data Raw: 61 62 6c 65 64 7b 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 30 30 37 62 66 66 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 30 30 37 62 66 66 7d 2e 62 74 6e 2d 70 72 69 6d 61 72 79 3a 6e 6f 74 28 3a 64 69 73 61 62 6c 65 64 29 3a 6e 6f 74 28 2e 64 69 73 61 62 6c 65 64 29 2e 61 63 74 69 76 65 2c 2e 62 74 6e 2d 70 72 69 6d 61 72 79 3a 6e 6f 74 28 3a 64 69 73 61 62 6c 65 64 29 3a 6e 6f 74 28 2e 64 69 73 61 62 6c 65 6 4 29 3a 61 63 74 69 76 65 2c 2e 73 68 6f 77 3e 2e 62 74 6e 2d 70 72 69 6d 61 72 79 2e 62 74 6f 70 64 6f 77 6e 2d 74 6f 6 7 67 6c 65 7b 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 30 30 36 32 63 63 3 b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 30 30 35 63 62 66 7d Data Ascii: abled{color:#fff;background-color:#007bff;border-color:#007bff}.btn-primary:not(:disabled):not(.disabled).ac tive,.btn-primary:not(:disabled):not(.disabled):active,.show>.btn-primary.dropdown-toggle{color:#fff;background-color:#0 062cc;border-color:#005cbf}
2022-07-01 14:30:01 UTC	67	IN	Data Raw: 3a 66 6f 63 75 73 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 30 20 30 20 2e 32 72 65 6d 20 72 67 62 61 28 34 30 2c 31 36 37 2c 36 39 2c 2e 35 29 7d 2e 62 74 6e 2d 73 75 63 63 65 73 73 2e 64 69 73 61 62 6c 65 64 2c 2e 62 74 6e 2d 73 75 63 63 65 73 73 3a 64 69 73 61 62 6c 65 64 7b 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 32 38 61 37 34 35 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 32 38 61 37 34 35 7d 2e 62 74 6e 2d 73 75 63 63 65 73 73 3a 6e 6f 74 28 3a 64 69 73 61 62 6c 65 64 29 3a 6e 6f 74 28 2e 64 69 73 61 62 6c 65 64 29 2e 61 63 74 69 76 65 2c 2e 62 74 6e 2d 73 75 63 63 65 73 73 3a 6e 6f 74 28 3a 64 69 73 61 62 6c 65 64 29 3a 6e 6f 74 28 2e 6 4 69 73 61 62 6c 65 64 29 3a 61 63 74 69 76 65 2c 2e 73 68 6f 77 Data Ascii: :focus{box-shadow:0 0 0 .2rem rgba(40,167,69,.5)}.btn-success.disabled,.btn-success:disabled{color:#fff;back ground-color:#28a745;border-color:#28a745}.btn-success:not(:disabled):not(.disabled).active,.btn-success:not(:disabled): not(.disabled):active,.show
2022-07-01 14:30:01 UTC	69	IN	Data Raw: 2e 62 74 6e 2d 77 61 72 6e 69 6e 67 2e 66 6f 63 75 73 2c 2e 62 74 6e 2d 77 61 72 6e 69 6e 67 3a 66 6f 63 75 73 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 30 20 30 20 2e 32 72 65 6d 20 72 67 62 61 28 32 35 35 2c 31 39 33 2c 37 2c 2e 35 29 7d 2e 62 74 6e 2d 77 61 72 6e 69 6e 67 2e 64 69 73 61 62 6c 65 64 2c 2e 62 74 6e 2d 77 61 72 6e 69 6e 67 3a 64 69 73 61 62 6c 65 64 7b 63 6f 6c 6f 72 3a 23 32 31 32 35 32 39 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 63 31 30 37 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 66 66 63 31 30 37 7d 2e 62 74 6e 2d 77 61 72 6e 6 9 6e 67 3a 6e 6f 74 28 3a 64 69 73 61 62 6c 65 64 29 3a 6e 6f 74 28 2e 64 69 73 61 62 6c 65 64 29 2e 61 63 74 69 76 65 2c 2e 62 74 6e 2d 77 61 72 6e 69 6e 67 3a 6e 6f 74 28 3a 64 69 73 Data Ascii: .btn-warning.focus,.btn-warning:focus{box-shadow:0 0 0 .2rem rgba(255,193,7,.5)}.btn-warning.disabled,.btn-w arning:disabled{color:#212529;background-color:#ffc107;border-color:#ffc107}.btn-warning:not(:disabled):not(.disabled).a ctive,.btn-warning:not(:dis
2022-07-01 14:30:01 UTC	70	IN	Data Raw: 3a 23 32 31 32 35 32 39 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 65 32 65 36 65 61 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 64 61 65 30 65 35 7d 2e 62 74 6e 2d 6c 69 67 68 74 2e 66 6f 63 75 73 2c 2e 62 74 6e 2d 6c 69 67 68 74 3a 66 6f 63 75 73 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 30 20 2e 32 72 65 6d 20 72 67 62 61 28 32 34 38 2c 32 34 39 2c 32 35 30 2c 2e 35 29 7d 2e 62 74 6e 2d 6c 69 67 68 74 2e 64 69 73 61 62 6c 65 64 2c 2e 62 74 6e 2d 6c 69 67 68 74 3a 64 69 73 61 62 6c 65 64 7b 63 6f 6c 6f 72 3a 23 32 31 32 35 32 39 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 38 66 39 66 61 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 66 38 66 39 66 61 7d 2e 62 74 6e 2d 6c 69 67 68 74 3a 6e 6f 74 28 3a 64 69 73 61 62 6c Data Ascii: :#212529;background-color:#e2e6ea;border-color:#dae0e5}.btn-light.focus,.btn-light:focus{box-shadow:0 0 0 .2rem rgba(248,249,250,.5)}.btn-light.disabled,.btn-light:disabled{color:#212529;background-color:#f8f9fa;border-color:#f8 f9fa}.btn-light:not(:disabl
2022-07-01 14:30:01 UTC	71	IN	Data Raw: 3a 6e 6f 6e 65 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 30 30 37 62 66 66 7d 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 70 72 69 6d 61 72 79 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 30 30 37 62 66 66 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 30 30 37 62 66 66 7d 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 70 72 69 6d 61 72 79 2e 66 6f 63 75 73 2c 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 70 72 69 6d 61 72 79 3a 66 6f 63 75 73 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 30 20 30 2e 32 72 65 6d 20 72 67 62 61 28 30 2c 31 32 33 2c 32 35 35 2c 2e 35 29 7d 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 70 72 69 6d 61 72 79 2e 64 69 73 61 62 6 c 65 64 2c 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 70 72 69 6d 61 Data Ascii: :none;border-color:#007bff}.btn-outline-primary:hover{color:#fff;background-color:#007bff;border-color:#007b ff}.btn-outline-primary.focus,.btn-outline-primary:focus{box-shadow:0 0 0 .2rem rgba(0,123,255,.5)}.btn-outline-primary. disabled,.btn-outline-prima
2022-07-01 14:30:01 UTC	73	IN	Data Raw: 64 7d 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 73 65 63 6f 6e 64 61 72 79 3a 6e 6f 74 28 3a 64 69 73 61 62 6c 65 64 29 3a 6e 6f 74 28 2e 64 69 73 61 62 6c 65 64 29 2e 61 63 74 69 76 65 3a 66 6f 63 75 73 2c 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 73 65 63 6f 6e 64 61 72 79 3a 6e 6f 74 28 3a 64 69 73 61 62 6c 65 64 29 3a 6e 6f 74 28 2e 64 69 73 61 62 6c 65 64 29 3a 61 63 74 69 76 65 3a 66 6f 63 75 73 2c 2e 73 68 6f 77 3e 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 73 65 63 6f 6e 64 61 72 79 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 3a 66 6f 63 75 73 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 30 20 2e 32 72 65 6d 20 72 67 62 61 28 31 30 38 2c 31 31 37 2c 31 32 35 2c 2e 35 29 7d 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 73 75 63 63 65 73 73 7b 63 6f 6c 6f 72 Data Ascii: d).btn-outline-secondary:not(:disabled):not(.disabled).active:focus,.btn-outline-secondary:not(:disabled):no t(.disabled):active:focus,.show>.btn-outline-secondary.dropdown-toggle:focus{box-shadow:0 0 0 .2rem rgba(108,1 17,125,.5)}.btn-outline-success{color
2022-07-01 14:30:01 UTC	74	IN	Data Raw: 2d 69 6e 66 6f 3a 64 69 73 61 62 6c 65 64 7b 63 6f 6c 6f 72 3a 23 31 37 61 32 62 38 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 74 72 61 6e 73 70 61 72 65 6e 74 7d 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 69 6e 66 6f 3a 6e 6f 74 28 3a 64 69 73 61 62 6c 65 64 29 3a 6e 6f 74 28 2e 64 69 73 61 62 6c 65 64 29 2e 61 63 74 69 76 65 2c 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 69 6e 66 6f 3a 6e 6f 74 28 3a 64 69 73 61 62 6c 65 64 29 3a 6e 6f 74 28 2e 64 69 73 61 62 6c 65 64 29 3a 61 63 74 69 76 65 2c 2e 73 68 6f 77 3e 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 69 6e 66 6f 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 7b 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 31 37 61 32 62 38 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f Data Ascii: -info:disabled{color:#17a2b8;background-color:transparent}.btn-outline-info:not(:disabled):not(.disabled).ac tive,.btn-outline-info:not(:disabled):not(.disabled):active,.show>.btn-outline-info.dropdown-toggle{color:#fff;background- color:#17a2b8;border-colo
2022-07-01 14:30:01 UTC	75	IN	Data Raw: 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 6e 6f 6e 65 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 64 63 33 35 34 35 7d 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 64 61 6e 67 65 72 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 66 66 66 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 64 63 33 35 34 35 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 64 63 33 35 34 35 7d 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 64 61 6e 67 65 72 3a 66 6f 63 75 73 7b 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 30 20 30 20 2e 32 72 65 6d 20 72 67 62 61 28 32 32 30 2c 35 33 2c 36 39 2c 2e 35 29 7d 2e 62 74 6e 2d 6f 75 74 6c 69 6e 65 2d 64 61 6e 67 65 72 2e 64 69 73 61 62 6c 65 64 2c 2e 62 74 6e 2d Data Ascii: ;background-image:none;border-color:#dc3545}.btn-outline-danger:hover{color:#fff;background-color: #dc3545;border-color:#dc3545}.btn-outline-danger.focus,.btn-outline-danger:focus{box-shadow:0 0 0 .2rem rgba(2 20,53,69,.5)}.btn-outline-danger.disabled,.btn-

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	136	IN	Data Raw: 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 6f 70 61 63 69 74 79 3a 2e 35 7d 2e 63 61 72 6f 75 73 65 6c 2d 63 6f 6e 74 72 6f 6c 2d 6e 65 78 74 3a 68 6f 76 65 72 2c 2e 63 61 72 6f 75 73 65 6c 2d 63 6f 6e 74 72 6f 6c 2d 70 72 65 76 3a 66 6f 63 75 73 2c 2e 63 61 72 6f 75 73 65 6c 2d 63 6f 6e 74 72 6f 6c 2d 70 72 65 76 3a 68 6f 76 65 72 7b 63 6f 6c 6f 72 3a 23 66 66 66 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 6f 75 74 6c 69 6e 65 3a 30 3b 6f 70 61 63 69 74 79 3a 2e 39 7d 2e 63 61 72 6f 75 73 65 6c 2d 63 6f 6e 74 72 6f 6c 2d 70 72 65 76 7b 6c 65 66 74 3a 30 7d 2e 63 61 72 6f 75 73 65 6c 2d 63 6f 6e 74 72 6f 6c 2d 6e 65 78 74 7b 72 69 67 68 74 3a 30 Data Ascii: t-align:center;opacity:.5}.carousel-control-next:focus,.carousel-control-next: hover,.carousel-control-prev:focus,.carousel-control-prev: hover{color:#fff;text-decoration:none;outline:0;opacity:.9}.carousel-control-prev{left:0}.carousel-control-next{right:0}
2022-07-01 14:30:01 UTC	140	IN	Data Raw: 74 7d 2e 62 6f 72 64 65 72 2d 6c 69 67 68 74 7b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 66 38 66 39 66 61 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 62 6f 72 64 65 72 2d 64 61 72 6b 7b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 33 34 33 61 34 30 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 62 6f 72 64 65 72 2d 67 68 69 74 65 7b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 66 66 66 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 72 6f 75 6e 64 65 64 7b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 2e 32 35 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 72 6f 75 6e 64 65 64 2d 74 6f 70 7b 62 6f 72 64 65 72 2d 74 6f 70 2d 6c 65 66 74 2d 72 61 64 69 75 73 3a 2e 32 35 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 3b 62 6f 72 64 65 72 2d 74 6f 70 2d 72 69 67 68 74 2d 72 61 64 69 75 73 3a 2e 32 35 72 65 Data Ascii: t}.border-light{border-color:#8f9fa!important}.border-dark{border-color:#343a40!important}.border-white{border-color:#fff!important}.rounded{border-radius:.25rem!important}.rounded-top{border-top-left-radius:.25rem!important;border-top-right-radius:.25rem}
2022-07-01 14:30:01 UTC	144	IN	Data Raw: 64 2d 72 65 73 70 6f 6e 73 69 76 65 2d 31 36 62 79 39 3a 3a 62 65 66 6f 72 65 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 35 36 2e 32 35 25 7d 2e 65 6d 62 65 64 2d 72 65 73 70 6f 6e 73 69 76 65 2d 34 62 79 33 3a 3a 62 65 66 6f 72 65 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 37 35 25 7d 2e 65 6d 62 65 64 2d 72 65 73 70 6f 6e 73 69 76 65 2d 31 62 79 31 3a 3a 62 65 66 6f 72 65 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 31 30 30 25 7d 2e 66 6c 65 78 2d 72 6f 77 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 69 65 6e 74 3a 68 6f 72 69 7a 6f 6e 74 61 6c 21 69 6d 70 6f 72 74 61 6e 74 3b 2d 6d 73 2d 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 72 6f 77 21 69 6d Data Ascii: d-responsive-16by9::before{padding-top:56.25%}.embed-responsive-4by3::before{padding-top:75%}.embed-responsive-1by1::before{padding-top:100%}.flex-row{-webkit-box-orient:horizontal!important;-webkit-box-direction:normal!important;-ms-flex-direction:row!important}
2022-07-01 14:30:01 UTC	148	IN	Data Raw: 74 61 72 74 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 70 61 63 6b 3a 73 74 61 72 74 21 69 6d 70 6f 72 74 61 6e 74 3b 2d 6d 73 2d 66 6c 65 78 2d 70 61 63 6b 3a 73 74 61 72 74 21 69 6d 70 6f 72 74 61 6e 74 3b 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 66 6c 65 78 2d 73 74 61 72 74 21 69 6d 70 6f 72 74 61 6e 74 3b 2d 6d 73 2d 66 6c 65 78 2d 63 6f 6e 74 65 6e 74 2d 73 6d 2d 65 6e 64 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 70 61 63 6b 3a 65 6e 64 21 69 6d 70 6f 72 74 61 6e 74 3b 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 66 6c 65 78 2d 65 6e 64 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 2d 73 6d 2d 63 65 6e 74 65 72 7b 2d 77 65 62 6b Data Ascii: tart{-webkit-box-pack:start!important;-ms-flex-pack:start!important;justify-content:flex-start!important}.justify-content-sm-end{-webkit-box-pack:end!important;-ms-flex-pack:end!important;justify-content:flex-end!important}.justify-content-sm-center{-webk
2022-07-01 14:30:01 UTC	152	IN	Data Raw: 6d 70 6f 72 74 61 6e 74 3b 2d 6d 73 2d 66 6c 65 78 2d 61 6c 69 67 6e 3a 62 61 73 65 6c 69 6e 65 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 61 6c 69 67 6e 2d 69 74 65 6d 73 2d 6d 64 2d 73 74 72 65 74 63 68 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 61 6c 69 67 6e 3a 73 74 72 65 74 63 68 21 69 6d 70 6f 72 74 61 6e 74 3b 2d 6d 73 2d 66 6c 65 78 2d 61 6c 69 67 6e 3a 73 74 72 65 74 63 68 21 69 6d 70 6f 72 74 61 6e 74 3b 61 6c 69 67 6e 2d 69 74 65 6d 70 6f 72 74 61 6e 74 3b 2d 6d 73 2d 66 6c 65 78 2d 61 6c 69 67 6e 2d 63 6f 6e 74 65 6e 74 2d 6d 64 2d 73 74 61 72 74 7b 2d 6d 73 2d 66 6c 65 78 2d 6c 69 6e 65 2d 70 61 63 6b 3a 73 74 61 72 74 21 69 6d 70 6f 72 74 61 6e 74 Data Ascii: mportant;-ms-flex-align:baseline!important;align-items:baseline!important}.align-items-md-stretch{-webkit-box-align:stretch!important;-ms-flex-align:stretch!important;align-items:stretch!important}.align-content-md-start{-ms-flex-line-pack:start!important}
2022-07-01 14:30:01 UTC	156	IN	Data Raw: 61 6e 74 3b 61 6c 69 67 6e 2d 73 65 6c 66 3a 66 6c 65 78 2d 65 6e 64 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 61 6c 69 67 6e 2d 73 65 6c 66 2d 6c 67 2d 63 65 6e 74 65 72 7b 2d 6d 73 2d 66 6c 65 78 2d 69 74 65 6d 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 21 69 6d 70 6f 72 74 61 6e 74 3b 61 6c 69 67 6e 2d 73 65 6c 66 3a 63 65 6e 74 65 72 21 69 6d 70 6f 72 74 61 6e 74 3b 61 6c 69 67 6e 2d 73 65 6c 66 2d 6c 67 2d 62 61 73 65 6c 69 6e 65 7b 2d 6d 73 2d 66 6c 65 78 2d 69 74 65 6d 2d 61 6c 69 67 6e 3a 62 61 73 65 6c 69 6e 65 21 69 6d 70 6f 72 74 61 6e 74 3b 61 6c 69 67 6e 2d 73 65 6c 66 3a 62 61 73 65 6c 69 6e 65 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 61 6c 69 67 6e 2d 73 65 6c 66 2d 6c 67 2d 73 74 72 65 74 63 68 7b 2d 6d 73 2d 66 6c 65 78 2d 69 74 65 6d 2d 61 6c 69 67 Data Ascii: ant;align-self:flex-end!important}.align-self-lg-center{-ms-flex-item-align:center!important;align-self:center!important}.align-self-lg-baseline{-ms-flex-item-align:baseline!important;align-self:baseline!important}.align-self-lg-stretch{-ms-flex-item-align
2022-07-01 14:30:01 UTC	160	IN	Data Raw: 6f 72 74 61 6e 74 7d 2e 70 6f 73 69 74 69 6f 6e 2d 72 65 6c 61 74 69 76 65 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 6f 73 69 74 69 6f 6e 2d 61 62 73 6f 6c 75 74 65 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 6f 73 69 74 69 6f 6e 2d 66 69 78 65 64 7b 70 6f 73 69 74 69 6f 6e 3a 66 69 78 65 64 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 6f 73 69 74 69 6f 6e 2d 73 74 69 63 6b 79 7b 70 6f 73 69 74 69 6f 6e 3a 2d 77 65 62 6b 69 74 2d 73 74 69 63 6b 79 21 69 6d 70 6f 72 74 61 6e 74 3b 70 6f 73 69 74 69 6f 6e 3a 73 74 69 63 6b 79 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 66 69 78 65 64 2d 74 6f 70 7b 70 6f 73 69 74 69 6f 6e 3a 66 69 78 65 64 3b 74 6f 70 3a 30 3b 72 69 67 68 Data Ascii: ortant}.position-relative{position:relative!important}.position-absolute{position:absolute!important}.position-fixed{position:fixed!important}.position-sticky{position:-webkit-sticky!important;position:sticky!important}.fixed-top{position:fixed;top:0;right
2022-07-01 14:30:01 UTC	163	IN	Data Raw: 33 61 30 31 0d 0a 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 2d 35 7b 70 61 64 64 69 6e 67 3a 33 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 79 2d 35 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 33 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 78 2d 35 7b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 33 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 62 2d 35 2c 2e 70 79 2d 35 7b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 33 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 6c 2d 35 2c 2e 70 78 2d 35 7b 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 33 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6d 2d 61 75 74 6f 7b 6d 61 72 67 69 6e 3a 61 75 74 6f 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6d 74 2d 61 75 74 6f 2c 2e 6d 79 2d 61 75 74 Data Ascii: 3a01em!important}.p-5{padding:3rem!important}.pt-5,.py-5{padding-top:3rem!important}.pr-5,.px-5{padding-right:3rem!important}.pb-5,.py-5{padding-bottom:3rem!important}.pl-5,.px-5{padding-left:3rem!important}.m-auto{margin:auto!important}.mt-auto,.my-aut

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	168	IN	Data Raw: 74 7d 2e 6d 72 2d 6d 64 2d 34 2c 2e 6d 78 2d 6d 64 2d 34 7b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 31 2e 35 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6d 62 2d 6d 64 2d 34 2c 2e 6d 79 2d 6d 64 2d 34 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 31 2e 35 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6d 6c 2d 6d 64 2d 34 2c 2e 6d 78 2d 6d 64 2d 34 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 2e 35 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6d 2d 6d 64 2d 35 7b 6d 61 72 67 69 6e 3a 33 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6d 74 2d 6d 64 2d 35 2c 2e 6d 79 2d 6d 64 2d 35 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 33 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 6d 72 2d 6d 64 2d 35 2c 2e 6d 78 2d 6d 64 2d 35 7b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 33 72 65 6d Data Ascii: t}.mr-md-4,.mx-md-4{margin-right:1.5rem!important}.mb-md-4,.my-md-4{margin-bottom:1.5rem!important}.ml-md-4,.mx-md-4{margin-left:1.5rem!important}.m-md-5{margin:3rem!important}.mt-md-5,.my-md-5{margin-top:3rem!important}.mr-md-5,.mx-md-5{margin-right:3rem
2022-07-01 14:30:01 UTC	172	IN	Data Raw: 2d 34 7b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 2e 35 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 6c 2d 6c 67 2d 34 2c 2e 70 78 2d 6c 67 2d 34 7b 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 31 2e 35 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 2d 6c 67 2d 35 7b 70 61 64 64 69 6e 67 3a 33 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 74 2d 6c 67 2d 35 2c 2e 70 79 2d 6c 67 2d 35 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 33 72 65 6d 21 69 6d 70 6f 7 2 74 61 6e 74 7d 2e 70 72 2d 6c 67 2d 35 2c 2e 70 78 2d 6c 67 2d 35 7b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 33 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 70 62 2d 6c 67 2d 35 2c 2e 70 79 2d 6c 67 2d 35 7b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 33 72 65 6d 21 69 6d 70 6f 72 74 61 6e 74 7d 2e Data Ascii: -4{padding-bottom:1.5rem!important}.pl-lg-4,.px-lg-4{padding-left:1.5rem!important}.p-lg-5{padding:3rem!important}.pt-lg-5,.py-lg-5{padding-top:3rem!important}.pr-lg-5,.px-lg-5{padding-right:3rem!important}.pb-lg-5,.py-lg-5{padding-bottom:3rem!important}.
2022-07-01 14:30:01 UTC	176	IN	Data Raw: 69 6d 70 6f 72 74 61 6e 74 7d 2e 74 65 78 74 2d 78 6c 2d 63 65 6e 74 65 72 7b 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 74 65 78 74 2d 6c 6f 77 65 72 63 61 73 65 7b 74 65 78 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 6c 6f 77 65 72 63 61 73 65 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 74 65 78 74 2d 75 70 70 65 72 63 61 73 65 7b 74 65 78 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 75 70 70 65 72 63 61 73 65 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 74 65 78 74 2d 63 61 70 69 74 61 6c 69 7a 65 7b 74 65 78 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 63 61 70 69 74 61 6c 69 7a 65 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 66 6f 6e 74 2d 77 65 69 67 68 74 2d 6c 69 67 68 74 7b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 33 30 30 21 69 6d 70 6f 72 74 61 6e 74 7d Data Ascii: important}.text-xl-center{text-align:center!important}.text-lowercase{text-transform:lowercase!important}.text-uppercase{text-transform:uppercase!important}.text-capitalize{text-transform:capitalize!important}.font-weight-light{font-weight:300!important}
2022-07-01 14:30:01 UTC	178	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49822	104.18.10.207	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	201	OUT	GET /bootstrap/4.0.0/js/bootstrap.min.js HTTP/1.1 Host: maxcdn.bootstrapcdn.com Connection: keep-alive Origin: https://eyecandylashcompany.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: script Referer: https://eyecandylashcompany.com/payment/frontend_paper_lantern/index.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	258	IN	HTTP/1.1 200 OK Date: Fri, 01 Jul 2022 14:30:01 GMT Content-Type: application/javascript; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding CDN-PullZone: 252412 CDN-Uid: b1941f61-b576-4f40-80de-5677acb38f74 CDN-RequestCountryCode: DE Access-Control-Allow-Origin: * Cache-Control: public, max-age=31919000 ETag: W/"14d449eb8876fa55e1ef3c2cc52b0c17" Last-Modified: Mon, 25 Jan 2021 22:04:04 GMT CDN-CachedAt: 03/10/2022 17:24:53 CDN-ProxyVer: 1.02 CDN-RequestPullCode: 200 CDN-RequestPullSuccess: True CDN-EdgeStorageId: 860 CDN-Status: 200 timing-allow-origin: * cross-origin-resource-policy: cross-origin X-Content-Type-Options: nosniff CDN-RequestId: fb4fb01b1e9c9f519dffab6f6c66766f CDN-Cache: HIT CF-Cache-Status: HIT Age: 43070 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Server: cloudflare CF-RAY: 723fd652cd029211-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-01 14:30:01 UTC	259	IN	Data Raw: 31 31 38 35 0d 0a 2f 2a 21 0a 20 20 2a 20 42 6f 6f 74 73 74 72 61 70 20 76 34 2e 30 2e 30 20 28 68 74 74 70 73 3a 2f 2f 67 65 74 62 6f 6f 74 73 74 72 61 70 2e 63 6f 6d 29 0a 20 20 2a 20 43 6f 70 79 72 69 67 68 74 20 32 30 31 31 2d 32 30 31 38 20 54 68 65 20 42 6f 6f 74 73 74 72 61 70 20 41 75 74 68 6f 72 73 20 28 68 74 74 70 73 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 74 77 62 73 2f 62 6f 6f 74 73 74 72 61 70 2f 67 72 61 70 68 73 2f 63 6f 6e 74 72 69 62 75 74 6f 72 73 29 0a 20 20 2a 20 4c 69 63 65 6e 73 65 64 20 75 6e 64 65 72 20 4d 49 54 20 28 68 74 74 70 73 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 74 77 62 73 2f 62 6f 6f 74 73 74 72 61 70 2f 62 6c 6f 62 2f 6d 61 73 74 65 72 2f 4c 49 43 45 4e 53 45 29 0a 20 20 2a 2f 0a 21 66 75 6e 63 74 69 6f 6e 28 74 Data Ascii: 1185/*! * Bootstrap v4.0.0 (https://getbootstrap.com) * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors) * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE) */!function(t
2022-07-01 14:30:01 UTC	259	IN	Data Raw: 65 6f 66 20 6d 6f 64 75 6c 65 3f 65 28 65 78 70 6f 72 74 73 2c 72 65 71 75 69 72 65 28 22 6a 71 75 65 72 79 22 29 2c 72 65 71 75 69 72 65 28 22 70 6f 70 70 65 72 2e 6a 73 22 29 29 3a 22 66 75 6e 63 74 69 6f 6e 22 3d 3d 74 79 70 65 6f 66 20 64 65 66 69 6e 65 26 26 64 65 66 69 6e 65 2e 61 6d 64 3f 64 65 66 69 6e 65 28 5b 22 65 78 70 6f 72 74 73 22 2c 22 6a 71 75 65 72 79 22 2c 22 70 6f 70 70 65 72 2e 6a 73 22 5d 2c 65 29 3a 65 28 74 2e 62 6f 6f 74 73 74 72 61 70 3d 7b 7d 2c 74 2e 6a 51 75 65 72 79 2c 74 2e 50 6f 70 70 65 72 29 7d 28 74 68 69 73 2c 66 75 6e 63 74 69 6f 6e 28 7 4 2c 65 2c 6e 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 69 28 74 2c 65 29 7b 66 6f 72 28 76 61 72 20 6e 3d 30 3b 6e 3c 65 2e 6c 65 6e 67 74 68 3b 6e 2b 2b Data Ascii: eof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)})(this,function(t,e,n){{"use strict";function i(t,e){for(var n =0;n<e.length;n++
2022-07-01 14:30:01 UTC	260	IN	Data Raw: 6c 65 6e 67 74 68 3e 30 3f 69 3a 6e 75 6c 6c 7d 63 61 74 63 68 28 74 29 7b 72 65 74 75 72 6e 20 6e 75 6c 6c 7d 7d 2c 72 65 66 6c 6f 77 3a 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 75 72 6e 20 74 2e 6f 66 66 73 65 74 48 65 69 67 68 74 7d 2c 74 72 69 67 67 65 72 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 3a 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 74 28 6e 29 2e 74 72 69 67 67 65 72 28 65 2e 65 6e 64 29 7d 2c 73 75 70 70 6f 72 74 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 42 6f 6f 6c 65 61 6e 28 65 29 7d 2c 69 73 45 6c 65 6d 65 6e 74 3a 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 75 72 6e 28 74 5b 30 5d 7c 7c 74 29 2e 6e 6f 64 65 54 79 70 65 7 d 2c 74 79 70 65 43 68 65 63 6b 43 6f 6e 66 69 67 3a 66 75 6e 63 Data Ascii: length>0?:!null}catch(t){return null}},reflow:function(t){return t.offsetHeight},triggerTransitionEnd:function(n){t(n).trigger(e.end)},supportsTransitionEnd:function(){return Boolean(e)},isElement:function(t){return(t[0] t).nodeType},typ eCheckConfig:func
2022-07-01 14:30:01 UTC	262	IN	Data Raw: 6e 74 28 74 29 2c 6e 3d 21 31 3b 72 65 74 75 72 6e 20 65 26 26 28 6e 3d 6f 28 65 29 5b 30 5d 29 2c 6e 7c 7c 28 6e 3d 6f 28 74 29 2e 63 6c 6f 73 65 73 74 28 22 2e 22 2b 66 29 5b 30 5d 29 2c 6e 7d 2c 65 2e 5f 74 72 69 67 67 65 72 43 6c 6f 73 65 45 76 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 65 3d 6f 2e 45 76 65 6e 74 28 75 2e 43 4c 4f 53 45 29 3b 72 65 74 75 72 6e 20 6f 28 74 29 2e 74 72 69 67 67 65 72 28 65 29 2c 65 7d 2c 65 2e 5f 72 65 6d 6f 76 65 45 6c 65 6d 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 65 3d 74 68 69 73 3b 6f 28 74 29 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 5f 29 2c 50 2e 73 75 70 70 6f 72 74 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 29 26 26 6f 28 74 29 2e 68 61 73 43 6c 61 73 73 28 64 29 3f 6f 28 74 Data Ascii: nt(t),n=!1;return e&&(n=o(e)[0]),n (n=o(t).closest("."+f)[0]),n,e._triggerCloseEvent=function(t){var e=o.E vent(u.CLOSE);return o(t).trigger(e),e,e._removeElement=function(t){var e=this;o(t).removeClass(_),P.supportsTransition End()&&o(t).hasClass(d)?o(t
2022-07-01 14:30:01 UTC	263	IN	Data Raw: 66 28 69 29 7b 69 66 28 22 72 61 64 69 6f 22 3d 3d 3d 69 2e 74 79 70 65 29 69 66 28 69 2e 63 68 65 63 6b 65 64 26 26 70 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 68 61 73 43 6c 61 73 73 28 43 29 29 74 3d 21 31 3b 65 6c 73 65 7b 76 61 72 20 73 0d 0a Data Ascii: f(t){if("radio"===i.type)if(i.checked&&p(this._element).hasClass(C))t=!1;else{var s

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	274	IN	Data Raw: 6c 7d 2c 69 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 73 3d 74 28 74 68 69 73 29 2c 6f 3d 73 2e 64 61 74 61 28 6e 29 2c 6c 3d 72 28 7b 7d 2c 61 2c 73 2e 64 61 74 61 28 29 2c 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 65 26 26 65 29 3b 69 66 28 21 6f 26 26 6c 2e 74 6f 67 67 6c 65 26 26 2f 73 68 6f 77 7c 68 69 64 65 2f 2e 74 65 73 74 28 65 29 26 26 28 6c 2e 74 6f 67 67 6c 65 3d 21 31 29 2c 6f 7c 7c 28 6f 6d 63 65 74 20 69 28 74 68 69 73 2c 6c 29 2c 73 2e 64 61 74 61 28 6e 2c 6f 29 29 2c 22 73 74 72 69 6e 67 22 3d 3d 74 79 70 65 6f 66 20 65 29 7b 69 66 28 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f Data Ascii: l,j,i_jQueryInterface=function(e){return this.each(function(){var s=t(this),o=s.data(n),l=r({j,a,s.data(),"object"==typeof e&&e});if(!o&&l.toggle&&show hide .test(e)&&(l.toggle=1),o (o=new i(this,l),s.data(n,o)),"string"==typeof e){if("undefined"==typeof
2022-07-01 14:30:01 UTC	275	IN	Data Raw: 6f 6d 2d 73 74 61 72 74 22 2c 53 3d 22 62 6f 74 74 6f 6d 2d 65 6e 64 22 2c 77 3d 22 72 69 67 68 74 2d 73 74 61 72 74 22 2c 4e 3d 22 6c 65 66 74 2d 73 74 61 72 74 22 2c 4f 3d 7b 6f 66 66 73 65 74 3a 30 2c 66 6c 69 70 3a 21 30 2c 62 6f 75 6e 64 61 72 79 3a 22 73 63 72 6f 6c 6c 50 61 72 65 6e 74 22 1d 2c 6b 3d 7b 6f 66 66 73 65 74 3a 22 28 6e 75 6d 62 65 72 7c 73 74 72 69 6e 67 7c 66 75 6e 63 74 69 6f 6e 29 22 2c 66 6c 69 70 3a 22 62 6f 6f 6c 65 61 6e 22 2c 62 6f 75 6e 64 61 72 79 3a 22 28 73 74 72 69 6e 67 7c 65 6c 65 6d 65 6e 74 29 22 7d 2c 4c 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 61 28 74 2c 65 29 7b 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 3d 74 2c 74 68 69 73 2e 5f 70 6f 70 70 65 72 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 63 6f 6e 66 Data Ascii: om-start",S="bottom-end",w="right-start",N="left-start",O={offset:0,flip:!0,boundary:"scrollParent"},k={offset:"(number string function)",flip:"boolean",boundary:"(string element)"},L=function(){function a(t,e){this._element=t,this._popper=null,this._conf
2022-07-01 14:30:01 UTC	276	IN	Data Raw: 65 6d 65 6e 74 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 6d 65 6e 75 3d 6e 75 6c 6c 2c 6e 75 6c 6c 21 3d 3d 74 68 69 73 2e 5f 70 6f 70 70 65 72 26 26 28 74 68 69 73 2e 5f 70 6f 70 70 65 72 2e 64 65 73 74 72 6f 79 28 29 2c 74 68 69 73 2e 5f 70 6f 70 70 65 72 3d 6e 75 6c 6c 29 7d 2c 6c 2e 75 70 64 61 74 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 68 69 73 2e 5f 69 6e 4e 61 76 62 61 72 3d 74 68 69 73 2e 5f 64 65 74 65 63 74 4e 61 76 62 61 72 28 29 2c 6e 75 6c 6c 21 3d 3d 74 68 69 73 2e 5f 70 6f 70 70 65 72 26 26 74 68 69 73 2e 5f 70 6f 70 70 65 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 65 3d 74 68 69 73 3b 74 28 74 68 69 73 2e 5f 65 6c 65 6d Data Ascii: ement=null,this._menu=null,null!==this._popper&&(this._popper.destroy(),this._popper=null)},l.update=function n(){this._inNavbar=this._detectNavbar(),null!==this._popper&&this._popper.scheduleUpdate()},l._addEventListeners=function(){var e=this;t(this._elem
2022-07-01 14:30:01 UTC	278	IN	Data Raw: 6c 29 2c 74 28 74 68 69 73 29 2e 64 61 74 61 28 69 2c 6e 29 29 2c 22 73 74 72 69 6e 67 22 3d 3d 74 79 70 65 6f 66 20 65 29 7b 69 66 28 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f 66 20 6e 5b 65 5d 74 68 72 6f 77 20 6e 65 77 20 54 79 70 65 45 72 72 6f 72 28 27 4e 6f 20 6d 65 74 68 6f 64 20 6e 61 6d 65 64 20 2d 27 2b 65 2b 27 2 2 27 29 3b 6e 5b 65 5d 28 29 7d 7d 29 7d 2c 61 2e 5f 63 6c 65 61 72 4d 65 6e 75 63 6d 75 6e 63 74 69 6f 6e 28 65 29 7b 69 66 28 21 65 7c 7c 33 21 3d 3d 65 2e 77 68 69 63 68 26 26 28 2d 6b 65 79 75 70 22 21 3d 3d 65 2e 74 79 70 65 7c 7c 39 3d 3d 3d 65 2e 77 68 69 63 68 29 29 66 6f 72 28 76 61 72 20 6e 3d 74 2e 6d 61 6b 65 41 72 72 61 79 28 74 28 45 29 29 2c 73 3d 30 3b 73 3c 6e 2e 6c 65 6e 67 74 68 3b 73 2b 2b 29 7b 76 Data Ascii: l),t(this).data(i,n)),"string"==typeof e){if("undefined"==typeof n[e])throw new TypeError("No method named "+e+"");n[e]()}}},a._clearMenus=function(e){if(!e 3!==e.which&&("keyup"===e.type 9===e.which))for(var n=t.makeArray(t(E)),s=0;s<n.length;s++){v
2022-07-01 14:30:01 UTC	279	IN	Data Raw: 3d 3d 3d 65 2e 77 68 69 63 68 26 26 72 3c 73 2e 6c 65 6e 67 74 68 2d 31 26 26 72 2b 2b 2c 72 3c 30 26 26 28 72 3d 30 29 2c 73 5b 72 5d 2e 66 6f 63 75 73 28 29 7d 7d 65 6c 73 65 7b 69 66 28 32 37 3d 3d 3d 65 2e 77 68 69 63 68 29 7b 76 61 72 20 6f 3d 74 28 6e 29 2e 66 69 6e 64 28 45 29 5b 30 5d 3b 74 28 6f 29 2e 74 72 69 67 67 65 72 28 22 6 6 6f 63 75 73 22 29 7d 74 28 74 68 69 73 29 2e 74 72 69 67 67 65 72 28 22 63 6c 69 63 6b 22 29 7d 7d 7d 2c 73 28 61 2c 6e 75 6c 6c 2c 5b 7b 6b 65 79 3a 22 56 45 52 53 49 4f 4e 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 22 34 2e 30 2e 30 2d 7d 7d 2c 7b 6b 65 79 3a 22 44 65 66 61 75 6c 74 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 4f 7d 7d 2c 7b 6b 65 79 3a 22 44 65 66 Data Ascii: ===e.which&&r<s.length-1&&r++,r<0&&(r=0),s[r].focus()}}else{if(27===e.which){var o=t(n).find(E)[0];t(o).trigger("focus");t(this).trigger("click")}}},s(a,null,{key:"VERSION",get:function(){return"4.0.0"}},{key:"Default",get:function(){return O}},{key:"Def
2022-07-01 14:30:01 UTC	280	IN	Data Raw: 67 67 6c 65 3d 22 6d 6f 64 61 6c 22 5d 27 2c 44 41 54 41 5f 44 49 53 4d 49 53 53 3a 27 5b 64 61 74 61 2d 64 69 73 6d 69 73 73 3d 22 6d 6f 64 61 6c 22 5d 27 2c 46 49 58 45 44 5f 43 4f 4e 54 45 4e 54 3a 22 2e 66 69 78 65 64 2d 74 6f 70 2c 20 2e 66 69 78 65 64 2d 62 6f 74 74 6f 6d 2c 20 2e 69 73 2d 66 69 78 65 64 2c 20 2e 73 74 69 63 6b 79 2d 74 6f 70 22 2c 53 54 49 43 4b 59 5f 43 4f 4e 54 45 4e 54 3a 22 2e 73 74 69 63 6b 79 2d 74 6f 70 22 2c 4e 41 56 42 41 52 5f 54 4f 47 47 4c 45 52 3a 22 2e 6e 61 76 62 61 72 2d 74 6f 67 67 6c 65 72 22 7d 2c 70 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 6f 28 65 2c 6e 29 7b 74 68 69 73 2e 5f 63 6f 6e 66 69 67 3d 74 68 69 73 2e 5f 67 65 74 43 6f 6e 66 69 67 28 6e 29 2c 74 68 69 73 2e 5f 65 6c 65 6d 65 6e Data Ascii: ggle="modal"],DATA_DISMISS:[data-dismiss="modal"],FIXED_CONTENT:".fixed-top,.fixed-bottom,.is-fixed,.sticky-top",STICKY_CONTENT:".sticky-top",NAVBAR_TOGGLER:".navbar-toggler"},p=function(){function o(e,n){this._config=this._getConfig(n),this._elemen
2022-07-01 14:30:01 UTC	282	IN	Data Raw: 3b 69 66 28 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 74 72 69 67 67 65 72 28 69 29 2c 74 68 69 73 2e 5f 69 73 53 68 6f 77 6e 26 26 21 69 2e 69 73 44 65 66 61 75 6c 74 50 72 65 76 65 6e 74 65 64 28 29 29 7b 74 68 69 73 2e 5f 69 73 53 68 6f 77 6e 3d 21 31 3b 76 61 72 20 73 3d 50 2e 73 75 70 70 6f 72 74 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 29 26 26 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 68 61 73 43 6c 61 73 73 28 64 29 3b 73 26 26 28 74 68 69 73 2e 5f 69 73 54 72 61 6e 73 69 74 69 6f 6e 69 6e 67 3d 21 30 29 2c 74 68 69 73 2e 5f 73 65 74 45 73 63 6 1 70 65 45 76 65 6e 74 28 29 2c 74 68 69 73 2e 5f 73 65 74 52 65 73 69 7a 65 45 76 65 6e 74 28 29 2c 74 28 64 6f 63 75 6d 65 6e 74 29 2e 6f 66 66 28 68 2e 46 4f 43 55 53 49 4e 29 2c 74 Data Ascii: ;if(t(this._element).trigger(i),this._isShown&&!isDefaultPrevented()){this._isShown=!1;var s=P.supportsTransitionEnd()&&t(this._element).hasClass(d);s&&(this._isTransitioning=!0),this._setEscapeEvent(),this._setResizeEvent(),t(document).off(h.FOCUSIN),t
2022-07-01 14:30:01 UTC	283	IN	Data Raw: 28 29 7b 6e 2e 5f 63 6f 6e 66 69 67 2e 66 6f 63 75 73 26 26 6e 2e 5f 65 6c 65 6d 65 6e 74 2e 66 6f 63 75 73 28 29 2c 6e 2e 5f 69 73 54 72 61 6e 73 69 74 69 6f 6e 69 6e 67 3d 21 31 2c 74 28 6e 2e 5f 65 6c 65 6d 65 6e 74 29 2e 74 72 69 67 67 65 72 48 73 29 7d 3b 69 3f 74 28 74 68 69 73 2e 5f 64 69 61 6c 6f 67 29 2e 6f 6e 65 28 50 2e 54 52 41 4e 53 49 54 49 4f 4e 5f 45 4e 44 2c 72 29 2e 65 6d 75 6c 61 74 65 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 33 30 30 29 3a 72 28 29 7d 2c 70 2e 5f 65 6e 66 6f 72 63 65 46 6f 63 75 73 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 65 3d 74 68 69 73 3b 74 28 64 6f 63 75 6d 65 6e 74 29 2e 6f 66 66 28 68 2e 46 4f 43 55 53 49 4e 29 2e 6f 6e 28 68 2e 46 4f 43 55 53 49 4e 2c 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 64 6f 63 75 6d Data Ascii:){n._config.focus&&n._element.focus(),n._isTransitioning=!1,t(n._element).trigger(s);i?t(this._dialog).one(P.TRANSITION_END,r).emulateTransitionEnd(300):r(),p._enforceFocus=function(){var e=this;t(document).off(h.FOCUSIN).on(h.FOCUSIN,function(n){docum

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	284	IN	Data Raw: 6b 64 72 6f 70 29 2e 61 70 70 65 6e 64 54 6f 28 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 29 2c 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 6f 6e 28 68 2e 43 4c 49 43 4b 5f 44 49 53 4d 49 53 53 2c 66 75 6e 63 74 69 6f 6e 28 74 29 7b 6e 2e 5f 69 67 6e 6f 72 65 42 61 63 6b 64 72 6f 70 43 6c 69 63 6b 3f 6e 2e 5f 69 67 6e 6f 72 65 42 61 63 6b 64 72 6f 70 43 6c 69 63 6b 3d 21 31 3a 74 2e 74 61 72 67 65 74 3d 3d 3d 74 2e 63 75 72 72 65 6e 74 54 61 72 67 65 74 26 28 22 73 74 61 74 69 63 22 3d 3d 3d 6e 2e 5f 63 6f 6e 66 69 67 2e 62 61 63 6b 64 72 6f 70 3f 6e 2e 5f 65 6c 65 6d 65 6e 74 2e 66 6f 63 75 73 28 29 3a 6e 2e 68 69 64 65 28 29 29 7d 29 2c 73 26 26 50 2e 72 65 66 6c 6f 77 28 74 68 69 73 2e 5f 62 61 63 6b 64 72 6f 70 29 2c 74 28 74 68 69 73 2e 5f 62 Data Ascii: kdrop).appendTo(document.body),t(this._element).on(h.CLICK_DISMISS,function(t){n._ignoreBackdropClick?n._ignoreBackdropClick=!1:t.target===t.currentTarget&&(!"static"===n._config.backdrop?n._element.focus():n.hide()))},s&&P.reflow(this._backdrop),t(this._b
2022-07-01 14:30:01 UTC	286	IN	Data Raw: 22 70 61 64 64 69 6e 67 2d 72 69 67 68 74 22 2c 73 29 2e 63 73 73 28 22 70 61 64 64 69 6e 67 2d 72 69 67 68 74 22 2c 70 61 72 73 65 46 6c 6f 61 74 28 72 29 2b 65 2e 5f 73 63 72 6f 6c 6c 62 61 72 57 69 64 74 68 2b 22 70 78 22 29 7d 29 2c 74 28 67 2e 53 54 49 43 4b 59 5f 43 4f 4e 54 45 4e 54 29 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 6e 2c 69 29 7b 76 61 72 20 73 3d 74 28 69 29 5b 30 5d 2e 73 74 79 6c 65 2e 6d 61 72 67 69 6e 52 69 67 68 74 2c 72 3d 74 28 69 29 2e 63 73 73 28 22 6d 61 72 67 69 6e 2d 72 69 67 68 74 22 29 3b 74 28 69 29 2e 64 61 74 61 28 22 6d 61 72 67 69 6e 2d 72 69 67 68 74 22 2c 73 29 2e 63 73 73 28 22 6d 61 72 67 69 6e 2d 72 69 67 68 74 22 2c 70 61 72 73 65 46 6c 6f 61 74 28 72 29 2d 65 2e 5f 73 63 72 6f 6c 6c 62 61 72 57 69 64 74 68 Data Ascii: "padding-right",s).css("padding-right",parseFloat(r)+e._scrollbarWidth+"px"));t(g.STICKY_CONTENT).each(function(n,i){var s=t(i)[0].style.marginRight,r=t(i).css("margin-right");t(i).data("margin-right",s).css("margin-right",parseFloat(r)-e._scrollbarWidth
2022-07-01 14:30:01 UTC	287	IN	Data Raw: 29 2e 64 61 74 61 28 6e 29 2c 61 3d 72 28 7b 7d 2c 6f 2e 44 65 66 61 75 6c 74 2c 74 28 74 68 69 73 29 2e 64 61 74 61 28 29 2c 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 65 26 26 65 29 3b 69 66 28 73 7c 7c 28 73 3d 6e 65 77 20 6f 28 74 68 69 73 2c 61 29 2c 74 28 74 68 69 73 29 2e 64 61 74 61 28 6e 2c 73 29 29 2c 22 73 74 72 69 6e 67 22 3d 3d 74 79 70 65 6f 66 20 65 29 7b 69 66 28 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f 66 20 73 5b 65 5d 29 74 68 72 6f 77 20 6e 65 77 20 54 79 70 65 45 72 72 6f 72 28 27 4e 6f 20 6d 65 74 68 6f 64 20 6e 61 6d 65 64 20 22 27 2b 65 2b 27 22 27 29 3b 73 5b 65 5d 28 69 29 7d 65 6c 73 65 20 61 2e 73 68 6f 77 26 26 73 2e 73 68 6f 77 28 69 29 7d 29 7d 2c 73 28 6f 2c 6e 75 6c 6c 2c 5b 7b 6b 65 79 3a 22 56 45 52 Data Ascii:).data(n),a=r({},o.Default,t(this).data()),"object"!==typeof e&&e;if(s (s=new o(this,a),t(this).data(n,s)),"string"!==typeof e){if("undefined"!==typeof s[e])throw new TypeError("No method named '"+e+"'");s[e]({})else a.show&&s.show({})},s({o,null,[{key:"VER
2022-07-01 14:30:01 UTC	288	IN	Data Raw: 75 3d 7b 61 6e 69 6d 61 74 69 6f 6e 3a 21 30 2c 74 65 6d 70 6c 61 74 65 3a 27 3c 64 69 76 20 63 6c 61 73 73 3d 22 74 6f 6f 6c 74 69 70 22 20 72 6f 6c 65 3d 22 74 6f 6f 6c 74 69 70 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 61 72 72 6f 77 22 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 74 6f 6f 6c 74 69 70 2d 69 6e 6e 65 72 22 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 27 2c 74 72 69 67 67 65 72 3a 22 68 6f 76 65 72 20 66 6f 63 75 73 22 6f 74 69 74 65 63 6a 22 22 2c 64 65 6c 61 79 3a 30 2c 68 74 6d 6c 3a 21 31 2c 73 65 6c 65 63 74 6f 72 3a 21 31 2c 70 6c 61 63 65 6d 65 6e 74 3a 22 74 6f 70 22 2c 6f 66 66 73 65 74 3a 30 2c 63 6f 6e 74 61 69 6e 65 72 3a 21 31 2c 66 61 6c 6c 62 61 63 6b 50 6c 61 63 65 6d 65 6e 74 3a 22 66 6c 69 70 22 2c 62 6f 75 6e 64 Data Ascii: u={animation:!0,template:'<div class="tooltip" role="tooltip"><div class="arrow"></div><div class="tooltip-inner"></div></div>',trigger:"hover focus",title:"",delay:0,html:!1,selector:!1,placement:"top",offset:0,container:!1,fallbackPlacement:"flip",bound
2022-07-01 14:30:01 UTC	290	IN	Data Raw: 6c 2c 69 29 7d 65 6c 73 65 7b 69 66 28 74 28 74 68 69 73 2e 67 65 74 54 69 70 45 6c 65 6d 65 6e 74 28 29 29 2e 68 61 73 43 6c 61 73 73 28 70 29 29 72 65 74 73 75 72 6e 20 76 6f 69 64 20 74 68 69 73 2e 5f 6c 65 61 76 65 28 6e 75 6c 6c 2c 74 68 69 73 29 3b 74 68 69 73 2e 5f 65 6e 74 65 72 28 6e 75 6c 6c 2c 74 68 69 73 29 7d 7d 2c 49 2e 64 69 73 70 6f 73 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 63 6c 65 61 72 54 69 6d 65 6f 75 74 28 74 68 69 73 2e 5f 74 69 6d 65 6f 75 74 29 2c 74 2e 72 65 6d 6f 76 65 44 61 74 61 28 74 68 69 73 2e 65 6c 65 6d 65 6e 74 2c 74 68 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 44 41 54 41 5f 4b 45 59 29 2c 74 28 74 68 69 73 2e 65 6c 65 6d 65 6e 74 29 2e 6f 66 66 28 74 68 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 45 56 45 4e 54 5f 4b Data Ascii: l,i)}else{if(t(t(this.getTipElement()).hasClass(p))return void this._leave(null,this);this._enter(null,this)),l.dispose=function(){clearTimeout(this._timeout),t.removeData(this.element,this.constructor.DATA_KEY),t(this.element).off(this.constructor.EVENT_K
2022-07-01 14:30:01 UTC	291	IN	Data Raw: 63 6f 6e 74 61 69 6e 73 28 74 68 69 73 2e 65 6c 65 6d 65 6e 74 2e 6f 77 6e 65 72 44 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2c 74 68 69 73 2e 74 69 70 29 7c 7c 74 28 72 29 2e 61 70 70 65 6e 64 54 6f 28 63 29 2c 74 28 74 68 69 73 2e 65 6c 65 6d 65 6e 74 29 2e 74 72 69 67 67 65 72 28 74 68 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 45 76 65 6e 74 2e 49 4e 53 45 52 54 45 44 29 2c 74 68 69 73 2e 5f 70 6f 70 65 72 3d 6e 65 77 20 6e 28 74 68 69 73 2e 65 6c 65 6d 65 6e 74 2c 72 2c 7b 70 6c 61 63 65 6d 65 6e 74 3a 68 2c 6d 6f 64 69 66 69 65 72 73 3a 7b 6f 66 66 73 65 74 3a 7b 6f 66 66 73 65 74 3a 74 68 69 73 2e 63 6f 6e 66 69 67 2e 6f 66 66 73 65 74 7d 2c 66 6c 69 70 3a 7b 62 65 68 61 76 69 6f 72 3a 74 68 69 73 2e 63 6f 6e 66 69 Data Ascii: contains(this.element.ownerDocument.documentElement,this.tip))t(r).appendTo(c),t(this.element).trigger(this.constructor.Event.INSERTED),this._popper=new n(this.element,r,{placement:h,modifiers:{offset:{offset:this.config.offset},flip:{behavior:this.conf
2022-07-01 14:30:01 UTC	292	IN	Data Raw: 69 6c 64 72 65 6e 28 29 2e 6f 66 66 28 22 6d 6f 75 73 65 6f 76 65 72 22 2c 6e 75 6c 6c 2c 74 2e 6e 6f 6f 70 29 2c 74 68 69 73 2e 5f 61 63 74 69 76 65 54 72 69 67 67 65 72 5b 79 5d 3d 21 31 2c 74 68 69 73 2e 5f 61 63 74 69 76 65 54 72 69 67 67 65 72 5b 45 5d 3d 21 31 2c 50 2e 73 75 70 70 6f 72 74 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 29 26 26 74 28 74 68 69 73 2e 74 69 70 29 2e 68 61 73 43 6c 61 73 73 28 67 29 3f 74 28 69 29 2e 6f 6e 65 28 50 2e 54 52 41 4e 53 49 54 49 4f 4e 5f 45 4e 44 2c 72 29 2e 65 6d 75 6c 61 74 65 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 31 35 30 29 3a 72 28 29 2c 74 68 69 73 2e 5f 68 6f 76 65 72 53 74 61 74 65 3d 22 22 29 7d 2c 49 2e 75 70 64 61 74 Data Ascii: ildren().off("mouseover",null,t.noop),this._activeTrigger[y]=!1,this._activeTrigger[T]=!1,this._activeTrigger[E]=!1,P.supportsTransitionEnd()&&t(this.tip).hasClass(g)?t(i).one(P.TRANSITION_END,r).emulateTransitionEnd(150):r(i),this._hoverState=""),l.update
2022-07-01 14:30:01 UTC	294	IN	Data Raw: 6e 73 74 72 75 63 74 6f 72 2e 45 76 65 6e 74 2e 46 4f 43 55 53 49 4e 2c 73 3d 6e 3d 3d 3d 45 3f 65 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 45 76 65 6e 74 2e 46 4f 43 55 53 4f 55 54 3b 74 28 65 2e 65 6c 65 6d 65 6e 74 29 2e 6f 6e 28 69 2c 65 2e 63 6f 6e 66 69 67 2e 73 65 6c 65 63 74 6f 72 2c 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 75 72 6e 20 65 2e 5f 65 6e 74 65 72 28 74 29 7d 29 2e 6f 6e 28 73 2c 65 2e 63 6f 6e 66 69 67 2e 73 65 6c 65 63 74 6f 72 2c 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 75 72 6e 20 65 2e 5f 6c 65 61 76 65 28 74 29 7d 29 7d 74 28 65 2e 65 6c 65 6d 65 6e 74 29 2e 63 6c 6f 73 65 73 74 28 22 2e 6d 6f 64 61 6c 22 29 2e 6f 6e 28 22 68 69 64 Data Ascii: nstructor.Event.FOCUSIN,s=!==E?e.constructor.Event.MOUSELEAVE:e.constructor.Event.FOCUSOUT;t(e.element).on(i,e.config.selector,function(t){return e._enter(t)}).on(s,e.config.selector,function(t){return e._leave(t)})(e.element).closest(".modal").on("hid

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	295	IN	Data Raw: 32 64 62 31 0d 0a 6c 65 67 61 74 65 43 6f 6e 66 69 67 28 29 29 2c 74 28 65 2e 63 75 72 72 65 6e 74 54 61 72 67 65 74 29 2e 64 61 74 61 28 69 2c 6e 29 29 2c 65 26 26 28 6e 2e 5f 61 63 74 69 76 65 54 72 69 67 67 65 72 5b 22 66 6f 63 75 73 6f 75 74 22 3d 3d 3d 65 2e 74 79 70 65 3f 54 3a 45 5d 3d 21 31 29 2c 6e 2e 5f 69 73 57 69 74 68 41 63 74 69 76 65 54 72 69 67 67 65 72 28 29 7c 7c 28 63 6c 65 61 72 54 69 6d 65 6f 75 74 28 6e 2e 5f 74 69 6d 65 6f 75 74 29 2c 6e 2e 5f 68 6f 76 65 72 53 74 61 74 65 3d 64 2c 6e 2e 63 6f 6e 66 69 67 2e 64 65 6c 61 79 26 26 6e 2e 63 6f 6e 66 69 67 2e 64 65 6c 61 79 2e 68 69 64 65 3f 6e 2e 5f 74 69 6d 65 6f 75 74 3d 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 2e 5f 68 6f 76 65 72 53 74 61 74 65 3d 3d 3d Data Ascii: 2db1legateConfig()),t(e.currentTarget).data(i,n)),e&&(n._activeTrigger["focusout"]===e.type?T:E)!=1),n._isWithActiveTrigger()) (clearTimeout(n._timeout),n._hoverState=d,n.config.delay&&n.config.delay.hide?n._timeout=setTimeout(function(){n._hoverState===
2022-07-01 14:30:01 UTC	296	IN	Data Raw: 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 6e 3d 74 28 74 68 69 73 29 2e 64 61 74 61 28 69 29 2c 73 3d 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 65 26 65 3b 69 66 28 6e 7c 7c 21 2f 64 69 73 70 6f 73 65 7c 68 69 64 65 2f 2e 74 65 73 74 28 65 29 29 26 26 28 6e 7c 7c 28 6e 3d 6e 65 77 20 61 28 74 68 69 73 2c 73 2 9 2c 74 28 74 68 69 73 29 2e 64 61 74 61 28 69 2c 6e 29 29 2c 22 73 74 72 69 6e 67 22 3d 3d 74 79 70 65 6f 66 20 65 29 29 7b 69 66 28 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f 66 20 6e 5b 65 5d 29 74 68 72 6f 77 20 6e 65 77 20 54 79 70 65 45 72 72 6f 72 28 27 4e 6f 20 6d 65 74 68 6f 64 20 6e Data Ascii: QueryInterface=function(e){return this.each(function(){var n=t(this).data(i),s="object"===typeof e&&e;if((n !dispose)hide/.test(e))&&(n (n=new a(this,s),t(this).data(i,n)),"string"===typeof e){if(("undefined"===typeof n[e])throw new TypeError('No method n
2022-07-01 14:30:01 UTC	298	IN	Data Raw: 3b 66 75 6e 63 74 69 6f 6e 20 70 28 29 7b 72 65 74 75 72 6e 20 72 2e 61 70 70 6c 79 28 74 68 69 73 2c 61 72 67 75 6d 65 6e 74 73 29 7c 7c 74 68 69 73 7d 67 3d 72 2c 28 6f 3d 70 29 2e 70 72 6f 74 6f 74 79 70 65 3d 4f 62 6a 65 63 74 2e 63 72 65 61 74 65 28 67 2e 70 72 6f 74 6f 74 79 70 65 29 2c 6f 2e 70 72 6f 74 6f 74 79 70 65 2e 63 6f 6e 73 74 72 75 63 74 6f 72 3d 6f 2c 6f 2e 5f 5f 70 72 6f 74 6f 5f 5f 3d 67 3b 76 61 72 20 6d 3d 70 2e 70 72 6f 74 6f 74 79 70 65 3b 72 65 74 75 72 6e 20 6d 2e 69 73 57 69 74 68 43 6f 6e 74 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 67 65 74 54 69 74 6c 65 28 29 7c 7c 74 68 69 73 2e 5f 67 65 74 43 6f 6e 74 65 6e 74 28 29 7d 2c 6d 2e 61 64 64 41 74 74 61 63 68 6d 65 6e 74 43 6c 61 73 73 3d Data Ascii: ,function p(){return r.apply(this,arguments)} this}g=r,(o=p).prototype=Object.create(g.prototype),o.prototype e.constructor=o,o._proto__=g;var m=p.prototype;return m.isWithContent=function(){return this.getTitle() this._getContent()}.m.addAttachmentClass=
2022-07-01 14:30:01 UTC	299	IN	Data Raw: 65 74 75 72 6e 20 5f 7d 7d 2c 7b 6b 65 79 3a 22 45 56 45 4e 54 5f 4b 45 59 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 69 7d 7d 2c 7b 6b 65 79 3a 22 44 65 66 61 75 6c 74 54 79 70 65 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 68 7d 7d 5d 29 2c 70 7d 28 55 29 3b 72 65 74 75 72 6e 20 74 2e 66 6e 5b 65 4d 3d 67 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 2c 74 2e 66 6e 5b 65 5d 2e 43 6f 6e 73 74 7 2 75 63 74 6f 72 3d 67 2c 74 2e 66 6e 5b 65 5d 2e 6e 6f 43 6f 6e 66 6c 69 63 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 6 5 74 75 72 6e 20 74 2e 66 6e 5b 65 5d 3d 6f 2c 67 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 7d 2c 67 7d 28 65 29 2c 4b 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 65 3d Data Ascii: eturn _}),{key:"EVENT_KEY",get:function(){return i}},{key:"DefaultType",get:function(){return h}}),p)(U);return t.fn[e]=g._jQueryInterface,t.fn[e].Constructor=g,t.fn[e].noConflict=function(){return t.fn[e]=o,g._jQueryInterface},g}(e),K=f unction(t){var e=
2022-07-01 14:30:01 UTC	300	IN	Data Raw: 69 67 2e 6d 65 74 68 6f 64 3f 6e 3a 74 68 69 73 2e 5f 63 6f 6e 66 69 67 2e 6d 65 74 68 6f 64 2c 73 3d 69 3d 3d 3d 5f 3f 74 68 69 73 2e 5f 67 65 74 53 63 72 6f 6c 6c 54 6f 70 28 29 3a 30 3b 74 68 69 73 2e 5f 6f 66 66 73 65 74 73 3d 5b 5d 2c 74 68 69 73 2e 5f 74 61 72 67 65 74 73 3d 5b 5d 2c 74 68 69 73 2e 5f 73 63 72 6f 6c 6c 48 65 69 67 68 74 3d 74 68 69 73 2e 5f 67 65 74 53 63 72 6f 6c 6c 48 65 69 67 68 74 28 29 2c 74 2e 6d 61 6b 65 41 72 72 61 79 28 74 28 74 68 69 73 2e 5f 73 65 6c 65 63 74 6f 72 29 29 2e 6d 61 70 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 6e 2c 72 3d 50 2e 67 65 74 53 65 6c 65 63 74 6f 72 46 72 6f 6d 45 6c 65 6d 65 6e 74 28 65 29 3b 69 66 28 72 26 26 28 6e 3d 74 28 72 29 5b 30 5d 29 2c 6e 29 7b 76 61 72 20 6f 3d 6e 2e 67 65 74 Data Ascii: ig.method?n:this._config.method,s!==_?this._getScrollTop():0;this._offsets=[],this._targets=[],this._scrollHeight=this._getScrollHeight(),t.makeArray(t(this._selector)).map(function(e){var n,r=P.getSelectorFromElement(e);if(r&&(n=t(r)[0]),n){var o=n.get
2022-07-01 14:30:01 UTC	302	IN	Data Raw: 2b 74 68 69 73 2e 5f 63 6f 6e 66 69 67 2e 6f 66 66 73 65 74 2c 65 3d 74 68 69 73 2e 5f 67 65 74 53 63 72 6f 6c 6c 48 65 69 67 68 74 28 29 2c 6e 3d 74 68 69 73 2e 5f 63 6f 6e 66 69 67 2e 6f 66 66 73 65 74 2b 65 2d 74 68 69 73 2e 5f 67 65 74 4f 66 66 73 65 74 48 65 69 67 68 74 28 29 3b 69 66 28 74 68 69 73 2e 5f 73 63 72 6f 6c 6c 48 65 69 67 68 74 21 3d 3d 65 26 26 74 68 69 73 2e 72 65 66 72 65 73 68 28 29 2c 74 3e 3d 6e 29 7b 76 61 72 20 69 3d 74 68 69 73 2e 5f 74 61 72 67 65 74 73 5b 74 68 69 73 2e 5f 74 61 72 67 65 74 73 2e 6c 65 6e 67 74 68 2d 31 5d 3b 74 68 69 73 2e 5f 61 63 74 69 76 65 54 61 72 67 65 74 21 3d 3d 69 26 26 74 68 69 73 2e 5f 61 63 74 69 76 61 74 65 28 69 29 7d 65 6c 73 65 7b 69 66 28 74 68 69 73 2e 5f 61 63 74 69 76 65 54 61 72 67 65 74 Data Ascii: +this._config.offset,e=this._getScrollHeight(),n=this._config.offset+e,this._getOffsetHeight());if(this._scrollHeight!==e&&this.refresh(),t>=n){var i=this._targets[this._targets.length-1];this._activeTarget!==i&&this._activate(i)}else{if(this._activeTarget
2022-07-01 14:30:01 UTC	303	IN	Data Raw: 29 7d 2c 73 28 6f 2c 6e 75 6c 6c 2c 5b 7b 6b 65 79 3a 22 56 45 52 53 49 4f 4e 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 22 34 2e 30 2e 30 22 7d 7d 2c 7b 6b 65 79 3a 22 44 65 66 61 75 6c 74 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 61 7d 7d 5d 29 2c 6f 7d 28 29 3b 72 65 74 75 72 6e 20 74 28 77 69 6e 64 6f 77 29 2e 6f 6e 28 68 2e 4c 4f 41 44 5f 44 41 54 41 5f 41 50 49 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 66 6f 72 28 76 61 72 20 65 3d 74 2e 6d 61 6b 65 41 72 72 61 79 28 74 28 66 2e 44 41 54 41 5f 53 50 59 29 2c 6e 3d 6 5 2e 6c 65 6e 67 74 68 3b 6e 2d 2d 3b 29 7b 76 61 72 20 69 3d 74 28 65 5b 6e 5d 29 3b 67 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 2e 63 61 6c 6c 28 69 2c 69 2e 64 61 74 61 28 Data Ascii:);},s(o,null,{key:"VERSION",get:function(){return"4.0.0"}},{key:"Default",get:function(){return a}}),o)},return t(window).on(h.LOAD_DATA_API,function(){for(var e=t.makeArray(t(f.DATA_SPY)),n=e.length;n--){var i=t(e[n]);g._jQueryInterface.call(i,i.data(
2022-07-01 14:30:01 UTC	304	IN	Data Raw: 64 28 29 29 7b 6f 26 26 28 6e 3d 74 28 6f 29 5b 30 5d 29 2c 74 68 69 73 2e 5f 61 63 74 69 76 61 74 65 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 2c 73 29 3b 76 61 72 20 67 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 6e 3d 74 2e 45 76 65 6e 74 28 72 2e 48 49 44 44 45 4e 2c 7b 72 65 6c 61 74 65 64 54 61 72 67 65 74 3a 65 2e 5f 65 6c 65 6d 65 6e 74 7d 29 2c 73 3d 74 2e 45 76 65 6e 74 28 72 2e 53 48 4f 57 4e 2c 7b 72 65 6c 61 74 65 64 54 61 72 67 65 74 3a 6 9 7d 29 3b 74 28 69 29 2e 74 72 69 67 67 65 72 28 6e 29 2c 74 28 65 2e 5f 65 6c 65 6d 65 6e 74 29 2e 74 72 69 67 67 65 72 28 73 29 7d 3b 6e 3f 74 68 69 73 2e 5f 61 63 74 69 76 61 74 65 28 6e 2c 6e 2e 70 61 72 65 6e 74 4e 6f 64 65 2c 67 29 3a 67 28 29 7d 7d 2c 69 2e 64 69 73 70 6f 73 65 3d 66 75 6e 63 Data Ascii: d()){o&&(n=(o)[0]),this._activate(this._element,s);var g=function(){var n=t.Event(r.HIDDEN,{relatedTarget:e._element}),s=t.Event(r.SHOWN,{relatedTarget:i});t(i).trigger(n),t(e._element).trigger(s);n?this._activate(n,n.parentNode,g):g()}}),i.dispose=func

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	306	IN	Data Raw: 6e 74 44 65 66 61 75 6c 74 28 29 2c 76 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 2e 63 61 6c 6c 28 74 28 74 68 69 73 29 2c 22 73 68 6f 77 22 29 7d 29 2c 74 2e 66 6e 2e 74 61 62 3d 76 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 2c 74 2e 66 6e 2e 74 61 62 2e 43 6f 6e 73 74 72 75 63 74 6f 72 3d 76 2c 74 2e 66 6e 2e 74 61 62 2e 6e 6f 43 6f 6e 66 6c 69 63 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 74 2e 66 6e 2e 74 61 62 3d 69 2 c 76 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 7d 2c 76 7d 28 65 29 3b 21 66 75 6e 63 74 69 6f 6e 28 74 29 7b 69 66 28 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f 66 20 74 29 74 68 72 6f 77 20 6e 65 77 20 54 79 70 65 45 72 72 6f 72 28 22 42 6f 6f 74 73 74 72 61 70 27 73 20 4a 61 76 61 Data Ascii: ntDefault(),v._jQueryInterface.call(t(this),"show"))),t.fn.tab=v._jQueryInterface,t.fn.tab.Constructor=v,t.f n.tab.noConflict=function(){return t.fn.tab=i,v._jQueryInterface},v}(e);!function(t){if("undefined"!==typeof t)throw new TypeError("Bootstrap's Java
2022-07-01 14:30:01 UTC	306	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49827	104.17.24.14	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	202	OUT	GET /ajax/libs/popper.js/1.12.9/umd/popper.min.js HTTP/1.1 Host: cdnjs.cloudflare.com Connection: keep-alive Origin: https://eyecandylashcompany.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: script Referer: https://eyecandylashcompany.com/payment/frontend_paper_lantern/index.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-07-01 14:30:01 UTC	307	IN	HTTP/1.1 200 OK Date: Fri, 01 Jul 2022 14:30:01 GMT Content-Type: application/javascript; charset=utf-8 Transfer-Encoding: chunked Connection: close Access-Control-Allow-Origin: * Cache-Control: public, max-age=30672000 ETag: W/"5eb03fa9-4af4" Last-Modified: Mon, 04 May 2020 16:15:37 GMT cf-cdnjs-via: cfworker/kv Cross-Origin-Resource-Policy: cross-origin Timing-Allow-Origin: * X-Content-Type-Options: nosniff Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" CF-Cache-Status: HIT Age: 1268063 Expires: Wed, 21 Jun 2023 14:30:01 GMT Report-To: {"endpoints":[{"url":"https://w.wa.nel.cloudflare.com/vreport/v3?s=KG4p7KBXyjpBWxuT1ekC9MKwR%2F0x4K rFM0Y%2BaPJM6K1FEJcS4jswbxt9K4r%2FjI4ASV13TBzRAFTEK4Lw377nWYKheTowH%2FztdGxLZ2EaH86SOIE dEllsHZFeLOzLulm7xlvU"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0.01,"report_to":"cf-nel","max_age":604800} Strict-Transport-Security: max-age=15780000 Server: cloudflare CF-RAY: 723fd652efbb9bd1-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-01 14:30:01 UTC	308	IN	Data Raw: 34 61 66 34 0d 0a 2f 2a 0a 20 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 46 65 64 65 72 69 63 6f 20 5a 69 76 6f 6c 6f 20 32 30 31 37 0a 20 44 69 73 74 72 69 62 75 74 65 64 20 75 6e 64 65 72 20 74 68 65 20 4d 49 54 20 4c 69 63 65 6e 73 65 20 28 6c 69 63 65 6e 73 65 20 74 65 72 6d 73 20 61 72 65 20 61 74 20 68 74 74 70 3a 2f 6f 70 65 6e 73 6f 75 72 63 65 2e 6f 72 67 2f 6c 69 63 65 6e 73 65 73 2f 4d 49 54 29 2e 0a 20 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 27 6f 62 6a 65 63 74 27 3d 3d 74 79 70 65 6f 66 20 65 78 70 6f 72 74 73 26 26 27 75 6e 64 65 66 69 6e 65 64 27 21 3d 74 79 70 65 6f 66 20 6d 6f 64 75 6c 65 3f 6d 6f 64 75 6c 65 2e 65 78 70 6f 72 74 73 3d 74 28 29 3a 27 66 75 6e 63 74 69 6f 6e 27 3d 3d 74 79 70 65 6f 66 20 64 65 66 69 6e 65 26 Data Ascii: 4af4/* Copyright (C) Federico Zivolo 2017 Distributed under the MIT License (license terms are at http://ope nsource.org/licenses/MIT). *(function(e,t){'object'===typeof exports&&'undefined'!=='module'?module.exports=t():'fun ction'===typeof define&
2022-07-01 14:30:01 UTC	308	IN	Data Raw: 72 3d 74 28 29 7d 29 28 74 68 69 73 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 27 75 73 65 20 73 74 72 69 63 74 27 3b 66 75 6e 63 74 69 6f 6e 20 65 28 65 29 7b 72 65 74 75 72 6e 20 65 26 26 27 5b 6f 62 6a 65 63 74 20 46 75 6e 63 74 69 6f 6e 5d 27 3d 3d 3d 7b 7d 2e 74 6f 53 74 72 69 6e 67 2e 63 61 6c 6c 28 65 29 7d 66 75 6e 63 74 69 6f 6e 20 74 28 65 2c 74 29 7b 69 66 28 31 21 3d 3d 65 2e 6e 6f 64 65 54 79 70 65 29 72 65 74 75 72 6e 5b 5d 3b 76 61 72 20 6f 3d 67 65 74 43 6f 6d 70 75 74 65 64 53 74 79 6c 65 28 65 2c 6e 75 6c 6c 29 3b 72 65 74 75 72 6e 20 74 3f 6f 5b 74 5d 3a 6f 7d 66 75 6e 63 74 69 6f 6e 20 6f 28 65 29 7b 72 65 74 75 72 6e 27 48 54 4d 4c 27 3d 3d 3d 65 2e 6e 6f 64 65 4e 61 6d 65 3f 65 3a 65 2e 70 61 72 65 6e 74 4e 6f 64 65 7c 7c 65 2e 68 6f 73 74 Data Ascii: r=t()))(this,function(){'use strict';function e(e){return e&&[object Function]==={}.toString.call(e)}function t(e,t){if(1!==(e.nodeType)?return[]:var o=getComputedStyle(e,null);return t[o[t]:o]function o(e){return'HTML'===e.nodeName? e:e.parentNode e.host

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	310	IN	Data Raw: 54 4d 4c 27 3d 3d 3d 69 29 7b 76 61 72 20 6e 3d 65 2e 6f 77 6e 65 72 44 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2c 72 3d 65 2e 6f 77 6e 65 72 44 6f 63 75 6d 65 6e 74 2e 73 63 72 6f 6c 6c 69 6e 67 45 6c 65 6d 65 6e 74 7c 7c 6e 3b 72 65 74 75 72 6e 20 72 5b 6f 5d 7d 72 65 74 75 72 6e 20 65 5b 6f 5d 7d 66 75 6e 63 74 69 6f 6e 20 6c 28 65 2c 74 29 7b 76 61 72 20 6f 3d 32 3c 61 72 67 75 6d 65 6e 74 73 2e 6c 65 6e 67 74 68 26 26 76 6f 69 64 20 30 21 3d 3d 61 72 67 75 6d 65 6e 74 73 5b 32 5d 26 26 61 72 67 75 6d 65 6e 74 73 5b 32 5d 2c 69 3d 61 28 74 2c 27 74 6f 70 27 29 2c 6e 3d 61 28 74 2c 27 6c 65 66 74 27 29 2c 72 3d 6f 3f 2d 31 3a 31 3b 72 65 74 75 72 6e 20 65 2e 74 6f 70 2b 3d 69 2a 72 2c 65 2e 62 6f 74 74 6f 6d 2b 3d 69 2a 72 Data Ascii: TML'===i){var n=e.ownerDocument.documentElement,r=e.ownerDocument.scrollingElement n;return r[o]}return e[o]}function l(e,t){var o=2<arguments.length&&void 0!==arguments[2]&&arguments[2],i=a(t,'top'),n=a(t,'left'),r=o?-1:1;return e.top+=i*r,e.bottom+=i*r}
2022-07-01 14:30:01 UTC	311	IN	Data Raw: 3d 27 48 54 4d 4c 27 3d 3d 3d 6f 2e 6e 6f 64 65 4e 61 6d 65 2c 70 3d 67 28 65 29 2c 73 3d 67 28 6f 29 2c 64 3d 6e 28 65 29 2c 61 3d 74 28 6f 29 2c 66 3d 70 61 72 73 65 46 6c 6f 61 74 28 61 2e 62 6f 72 64 65 72 54 6f 70 57 69 64 74 68 2c 31 30 29 2c 6d 3d 70 61 72 73 65 46 6c 6f 61 74 28 61 2e 62 6f 72 64 65 72 4c 65 66 74 57 69 64 74 68 2c 31 30 29 2c 68 3d 63 28 7b 74 6f 70 3a 70 2e 74 6f 70 2d 73 2e 74 6f 70 2d 66 2c 6c 65 66 74 3a 70 2e 6c 65 66 74 2d 73 2e 6c 65 66 74 2d 6d 2c 77 69 64 74 68 3a 70 2e 77 69 64 74 68 2c 68 65 69 67 68 74 3a 70 2e 68 65 69 67 68 74 7d 29 3b 69 66 28 68 2e 6d 61 72 67 69 6e 54 6f 70 3d 30 2c 68 2e 6d 61 72 67 69 6e 4c 65 66 74 3d 30 2c 21 69 26 26 72 29 7b 7 6 61 72 20 75 3d 70 61 72 73 65 46 6c 6f 61 74 28 61 2e 6d 61 72 Data Ascii: ="HTML"===o.nodeName,p=g(e),s=g(o),d=n(e),a=t(o),f=parseFloat(a.borderTopWidth,10),m=parseFloat(a.borderLeftWidth,10),h=c({top:p.top-s.top-f,left:p.left-s.left-m,width:p.width,height:p.height}):if(h.marginTop=0,h.margi nLeft=0,li&&r){var u=parseFloat(a.mar
2022-07-01 14:30:01 UTC	312	IN	Data Raw: 66 28 2d 31 3d 3d 3d 65 2e 69 6e 64 65 78 4f 66 28 27 61 75 74 6f 27 29 29 72 65 74 75 72 6e 20 65 3b 76 61 72 20 70 3d 79 28 6f 2c 69 2c 72 2c 6e 29 2c 73 3d 7b 74 6f 70 3a 7b 77 69 64 74 68 3a 70 2e 77 69 64 74 68 2c 68 65 69 67 68 74 3a 74 2e 74 6f 70 2d 70 2e 74 6f 70 7d 2c 72 69 67 68 74 3a 7b 77 69 64 74 68 3a 70 2e 72 69 67 68 74 2d 74 2e 72 69 67 68 74 2c 68 65 69 67 68 74 3a 70 2e 68 65 69 67 68 74 7d 2c 62 6f 74 74 6f 6d 3a 7b 77 69 64 74 68 3a 7 0 2e 77 69 64 74 68 2c 68 65 69 67 68 74 3a 70 2e 62 6f 74 74 6f 6d 74 74 6f 6d 74 2c 6e 65 66 74 6f 6d 74 6f 6d 74 68 3a 74 2e 6c 65 66 74 2d 70 2e 6c 65 66 74 2c 68 65 69 67 68 74 3a 70 2e 68 65 69 67 68 74 7d 7d 2c 64 3d 4f 62 6a 65 63 74 2e 6b 65 79 73 28 73 29 2e 6d 61 70 28 66 75 6e Data Ascii: f(-1===e.indexOf('auto'))return e;var p=y(o,i,r,n),s={top:{width:p.width,height:t.top-p.top},right:{width:p.right-t.righ t,height:p.height},bottom:{width:p.width,height:p.bottom-t.bottom},left:{width:t.left-p.left,height:p.height}};d=Objec t.keys(s).map(fun
2022-07-01 14:30:01 UTC	314	IN	Data Raw: 65 2e 69 6e 64 65 78 4f 66 28 69 29 7d 66 75 6e 63 74 69 6f 6e 20 43 28 74 2c 6f 2c 69 29 7b 76 61 72 20 6e 3d 76 6f 69 64 20 30 3d 3d 3d 69 3f 74 3a 74 2e 73 6c 69 63 65 28 30 2c 44 28 74 2c 27 6e 61 6d 65 27 2c 69 29 29 3b 72 65 74 75 72 6e 20 6e 2e 66 6f 72 45 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 74 29 7b 74 5b 27 66 75 6e 63 74 69 6f 6e 27 5d 26 26 63 6f 6e 73 6f 6c 65 2e 77 61 72 6e 28 27 60 6d 6f 64 69 66 69 65 72 2e 66 75 6e 63 74 69 6f 6e 60 20 69 73 20 64 65 70 72 65 63 61 74 65 64 2c 20 75 73 65 20 60 6d 6f 64 69 66 69 65 72 2e 66 6e 60 21 27 29 3b 76 61 72 20 69 3d 74 5b 27 66 75 6e 63 74 69 6f 6e 27 5d 7c 7c 74 2e 66 6e 3b 74 2e 65 6e 61 62 6c 65 64 26 26 65 28 69 29 26 26 28 6f 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 3d 63 28 6f 2e 6f Data Ascii: e.indexOf(i))function C(t,o,i){var n=void 0===i?t.slice(0,D(t,'name',i));return n.forEach(function(t){t['function']& &console.warn("`modifier.function` is deprecated, use `modifier.fn`!");var i=t['function'] t.fn;t.enabled&&e(i)&&(o.off sets.popper=c(o.o
2022-07-01 14:30:01 UTC	315	IN	Data Raw: 2c 74 68 69 73 2e 70 6f 70 70 65 72 2e 73 74 79 6c 65 2e 70 6f 73 69 74 69 6f 6e 3d 27 27 2c 74 68 69 73 2e 70 6f 70 65 72 2e 73 74 79 6c 65 2e 74 6f 70 3d 27 2c 74 68 69 73 2e 70 6f 70 65 72 2e 73 74 79 6c 65 5b 57 28 27 74 72 61 6e 73 66 6f 72 6d 27 29 5d 3d 27 27 29 2c 74 68 69 73 2e 64 69 73 61 62 6c 65 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 73 28 29 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 72 65 6d 6f 76 65 4f 6e 44 65 73 74 72 6f 79 26 26 74 68 69 73 2e 70 6f 70 70 65 72 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 72 65 6d 6f 76 65 43 68 69 6c 64 28 74 68 69 73 2e 70 6f 70 70 65 72 29 2c 74 68 69 73 7d 66 75 6e 63 74 69 6f 6e 20 42 28 65 29 7b 76 61 72 20 74 3d 65 2e 6f 77 6e 65 72 44 6f 63 75 6d 65 6e 74 3b 72 65 74 75 72 6e 20 74 3f 74 2e 64 65 Data Ascii: .this.popper.style.position=",this.popper.style.top=",this.popper.style[W('transform')]=""),this.disableEventListener s(rs),this.options.removeOnDestroy&&this.popper.parentNode.removeChild(this.popper),this}function B(e){var t=e.ownerDocument;return t?!.de
2022-07-01 14:30:01 UTC	316	IN	Data Raw: 6e 28 6f 29 7b 76 61 72 20 69 3d 74 5b 6f 5d 3b 21 31 3d 3d 3d 69 3f 65 2e 72 65 6d 6f 76 65 41 74 74 72 69 62 75 74 65 28 6f 2c 74 5b 6f 5d 29 7d 29 7d 66 75 6e 63 74 69 6f 6e 20 46 28 65 2c 74 2c 6f 29 7b 76 61 72 20 69 3d 54 28 65 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 6f 3d 65 2e 6e 61 6d 65 3b 72 65 74 75 72 6e 20 6f 3d 3d 3d 74 7d 29 2c 6e 3d 21 21 69 26 26 6e 65 28 65 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 65 2e 6e 61 6d 65 3d 3d 3d 6f 26 26 65 2e 65 6e 61 62 6c 65 64 26 26 6 5 2e 6f 72 64 65 72 3c 69 2e 6f 72 64 65 72 7d 29 3b 69 66 28 21 6e 29 7b 76 61 72 20 72 3d 27 60 27 2b 74 2b 27 60 27 3b 63 6f 6e 73 6f 6c 65 2e 77 61 72 6e 28 27 60 27 2b 6f 2b 27 60 Data Ascii: n(o){var i=t[o];1!==i?e.removeAttribute(o):e.setAttribute(o,t[o])}}function F(e,t,o){var i=T(e,function(e){var o=e.name;return o===t}),n=!li&&e.some(function(e){return e.name===o&&e.enabled&&e.order<i.order});if(!n){var r=""+"t+"";console.warn("`"+o+"`
2022-07-01 14:30:01 UTC	318	IN	Data Raw: 63 6f 6e 63 61 74 28 70 2e 73 6c 69 63 65 28 73 2b 31 29 29 5d 3b 72 65 74 75 72 6e 20 61 3d 61 2e 6d 61 70 28 66 75 6e 63 74 69 6f 6e 28 65 2c 69 29 7b 76 61 72 20 6e 3d 28 31 3d 3d 3d 69 3f 21 72 3a 72 29 3f 27 68 65 69 67 68 74 27 3a 27 77 69 64 74 68 27 2c 70 3d 21 31 3b 72 65 74 75 72 6e 20 65 2e 72 65 64 75 63 65 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 72 65 74 75 72 6e 27 27 3d 3d 3d 65 5b 65 2e 6c 65 6e 67 74 68 2d 31 5d 26 26 2d 31 21 3d 3d 5b 27 2b 27 2c 27 2d 27 5d 2e 69 6e 64 65 78 4f 66 28 74 29 3f 28 65 5b 65 2e 6c 65 6e 67 74 68 2d 31 5d 3d 74 2c 70 3d 21 30 2c 65 29 3a 70 3f 28 65 5b 65 2e 6c 65 6e 67 74 68 2d 31 5d 2b 3d 74 2c 70 3d 21 31 2c 65 29 3a 65 2e 63 6f 6e 63 61 74 28 74 29 7d 2c 5b 5d 29 2e 6d 61 70 28 66 75 6e 63 74 69 6f Data Ascii: concat(p.slice(s+1));return a=a.map(function(e,i){var n=(1===i?r:r)?'height':'width',p=1;return e.reduce(function(e,t){return"===e.length-1)&&-1!=[+',',-'].indexOf(t)?(e[e.length-1]=t,p=10,e):p?(e[e.length-1]+=t,p=11,e):e.concat(t),[]}).map(function
2022-07-01 14:30:01 UTC	319	IN	Data Raw: 65 3d 6f 2e 65 6e 75 6d 65 72 61 62 6c 65 7c 7c 21 31 2c 6f 2e 63 6f 6e 66 69 67 75 72 61 62 6c 65 3d 21 30 2c 27 76 61 6c 75 65 27 69 6e 20 6f 26 26 28 6f 2e 77 72 69 74 61 62 6c 65 3d 21 30 29 2c 4f 62 6a 65 63 74 2e 64 65 66 69 6e 65 50 72 6f 70 65 72 74 79 28 65 2c 6f 2e 6b 65 79 2c 6f 29 7d 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 74 2c 6f 2c 69 29 7b 72 65 74 75 72 6e 20 6f 26 26 65 28 74 2e 70 72 6f 74 6f 74 79 70 65 2c 6f 29 2c 69 26 26 65 28 74 2c 69 29 2c 74 7d 7d 28 29 2c 70 65 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6f 29 7b 72 65 74 75 72 6e 20 74 20 69 6e 20 65 3f 4f 62 6a 65 63 74 2e 64 65 66 69 6e 65 50 72 6f 70 65 72 74 79 28 65 2c 74 2c 7b 76 61 6c 75 65 3a 6f 2c 65 6e 75 6d 65 72 61 62 6c 65 3a 21 30 2c 63 6f 6e 66 69 67 75 72 Data Ascii: e=o.enumerable 1,o.configurable=!0,value'in o&&(o.writable=!0),Object.defineProperty(e,o.key,o)}return fu nction(t,o,i){return o&&(t.prototype,o),i&&(t,i),t}(),pe=function(e,t,o){return t in e?Object.defineProperty(e,t,{val ue:o,enumerable:!0,configur

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	320	IN	Data Raw: 6f 64 69 66 69 65 72 73 5b 65 5d 29 7d 29 2e 73 6f 72 74 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 72 65 74 75 72 6e 20 65 2e 6f 72 64 65 72 2d 74 2e 6f 72 64 65 72 7d 29 2c 74 68 69 73 2e 6d 6f 64 69 66 69 65 72 73 2e 66 6f 72 45 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 74 29 7b 74 2e 65 6e 61 62 6c 65 64 26 26 65 28 74 2e 6f 6e 4c 6f 61 64 29 26 26 74 2e 6f 6e 4c 6f 61 64 28 6e 2e 72 65 66 65 72 65 6e 63 65 2c 6e 2e 70 6f 70 70 65 72 2c 6e 2e 6f 70 74 69 6f 6e 73 2c 74 2c 6e 2e 73 74 61 74 65 29 7d 29 2c 74 68 69 73 2e 75 70 64 61 74 65 28 29 3b 76 61 72 20 70 3d 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 65 76 65 6e 74 73 45 6e 61 62 6c 65 64 3b 70 26 26 74 68 69 73 2e 65 6e 61 62 6c 65 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 73 28 29 2c 74 68 69 73 2e 73 Data Ascii: odifiers[e]])).sort(function(e,t){return e.order-t.order})),this.modifiers.forEach(function(t){t.enabled&&e(t.onLoad)&&t.onLoad(n.reference,n.popper,n.options,t.n.state)})),this.update();var p=this.options.eventsEnabled;p&&this.enableEventListeners(),this.s
2022-07-01 14:30:01 UTC	322	IN	Data Raw: 69 6f 6e 28 65 29 7b 76 61 72 20 6f 3d 70 5b 65 5d 3b 72 65 74 75 72 6e 20 70 5b 65 5d 3c 69 5b 65 5d 26 26 21 74 2e 65 73 63 61 70 65 57 69 74 68 52 65 66 65 72 65 6e 63 65 26 26 28 6f 3d 4a 28 70 5b 65 5d 2c 69 5b 65 5d 29 29 2c 70 65 28 7b 7d 2c 65 2c 6f 29 7d 2c 73 65 63 6f 6e 64 61 72 79 3a 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 6f 3d 27 72 69 67 68 74 27 3d 3d 65 3f 27 6c 65 66 74 27 3a 27 74 6f 70 27 2c 6e 3d 70 5b 6f 5d 3b 72 65 74 75 72 6e 20 70 5b 65 5d 3e 69 5b 65 5d 26 26 21 74 2e 65 73 63 61 70 65 57 69 74 68 52 65 66 65 72 65 6e 63 65 26 26 28 6e 3d 5f 28 70 5b 6f 5d 2c 69 5b 65 5d 2d 28 27 72 69 67 68 74 27 3d 3d 65 3f 70 2e 77 69 64 74 68 3a 70 2e 68 65 69 67 6 8 74 29 29 29 2c 70 65 28 7b 7d 2c 6f 2c 6e 29 7d 7d 3b 72 65 74 Data Ascii: ion(e){var o=p[e];return p[e]<i[e]&&!t.escapeWithReference&&(o=J(p[e],i[e])),pe({},e,o)},secondary:function(e){var o='right'===e?'left':'top',n=p[o];return p[e]>i[e]&&!t.escapeWithReference&&(n=_(p[o],i[e]-('right'===e?p.width:p.height))),pe({},o,n)}};ret
2022-07-01 14:30:01 UTC	323	IN	Data Raw: 67 5d 2d 75 29 29 2c 64 5b 6d 5d 2b 75 3e 73 5b 67 5d 26 26 28 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 5b 6d 5d 2b 3d 64 5b 6d 5d 2b 75 2d 73 5b 67 5d 29 2c 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 3d 63 28 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 29 3b 76 61 72 20 62 3d 64 5b 6d 5d 2b 64 5b 6c 5d 2f 32 2d 75 2f 32 2c 77 3d 74 28 65 2e 69 6e 73 74 61 6e 63 65 2e 70 6f 70 70 65 72 29 2c 79 3d 70 61 72 73 65 46 6c 6f 61 74 28 77 5b 27 6d 61 72 67 69 6e 27 2b 66 5d 2c 31 30 29 2c 45 3d 70 61 72 73 65 46 6c 6f 61 74 28 77 5b 27 62 6f 72 64 65 72 27 2b 66 2 b 27 57 69 64 74 68 27 5d 2c 31 30 29 2c 76 3d 62 2d 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 5b 6d 5d 2d 79 2d 45 3b 72 65 74 75 72 6e 20 76 3d 4a 28 5f 28 73 5b 6c 5d 2d 75 2c Data Ascii: g]-u)),d[m]+u>s[g]&&(e.offsets.popper[m]+-d[m]+u-s[g]),e.offsets.popper=c(e.offsets.popper);var b=d[m]+d[l]/2-u/2,w=t(e.instance.popper),y=parseFloat(w['margin'+f],10),E=parseFloat(w['border'+f+'Width'],10),v=b-e.offsets.popper[m]-y-E;return v=J(_(s[l],-u,
2022-07-01 14:30:01 UTC	324	IN	Data Raw: 3b 28 6d 7c 7c 62 7c 7c 79 29 26 26 28 65 2e 66 6c 69 70 70 65 64 3d 21 30 2c 28 6d 7c 7c 62 29 26 26 28 69 3d 70 5b 64 2b 31 5d 29 2c 79 26 26 28 72 3d 4b 28 72 29 29 2c 65 2e 70 6c 61 63 65 6d 65 6e 74 3d 69 2b 28 72 3f 27 2d 27 2b 72 3a 27 27 29 2c 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 3d 73 65 28 7b 7d 2c 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 2c 53 28 65 2e 69 6e 73 74 61 6e 63 65 2e 70 6f 70 70 65 72 2c 65 2e 6f 66 66 73 65 74 73 2e 72 65 66 65 72 65 6e 63 65 2c 65 2e 70 6c 61 63 65 6d 65 6e 74 29 29 2c 65 3d 43 28 65 2e 69 6e 73 74 61 6e 63 65 2e 6d 6f 64 69 66 69 65 72 73 2c 65 2c 27 66 6c 69 70 27 29 29 7d 29 2c 65 7d 2c 62 65 68 61 76 69 6f 72 3a 27 66 6c 69 70 27 2c 70 61 64 64 69 6e 67 3a 35 2c 62 6f 75 6e 64 61 72 69 65 73 Data Ascii: :(m b y)&&(e.flipped=!0,(m b)&&(i=p[d+1]),y&&(r=K(r)),e.placement=i+(r?'-'+r:'),e.offsets.popper=se({},e.offsets.popper,S(e.instance.popper,e.offsets.reference,e.placement)),e=C(e.instance.modifiers,e,'flip'))),e),behavior:'flip',padding:5,boundaries
2022-07-01 14:30:01 UTC	326	IN	Data Raw: 72 28 65 2e 69 6e 73 74 61 6e 63 65 2e 70 6f 70 70 65 72 29 2c 66 3d 67 28 6c 29 2c 6d 3d 7b 70 6f 73 69 74 69 6f 6e 3a 6e 2e 70 6f 73 69 74 69 6f 6e 7d 2c 68 3d 7b 6c 65 66 74 3a 58 28 6e 2e 6c 65 66 74 29 2c 74 6f 70 3a 58 28 6e 2e 74 6f 70 29 2c 62 6f 74 74 6f 6d 3a 58 28 6e 2e 62 6f 74 74 6f 6d 29 2c 72 69 67 68 74 3a 58 28 6e 2e 72 69 67 68 74 29 7d 2c 63 3d 27 62 6f 74 74 6f 6d 27 3d 3d 3d 6f 3f 27 74 6f 70 27 3a 27 62 6f 74 74 6f 6d 27 2c 75 3d 27 72 69 67 68 74 27 3d 3d 3d 69 3f 27 6c 65 66 74 27 3a 27 72 69 67 68 74 27 2c 62 3d 57 28 27 74 72 61 6e 73 66 6f 72 6d 27 29 3b 69 66 28 64 3d 27 62 6f 74 74 6f 6d 27 3d 3d 63 3f 2d 66 2e 68 65 69 67 68 74 2b 68 2e 62 6f 74 74 6f 6d 3a 68 2e 74 6f 70 2c 73 3d 27 72 69 67 68 74 27 3d 3d 75 3f 2d 66 2e 77 Data Ascii: r(e.instance.popper),f=g(l),m={position:n.position},h={left:X(n.left),top:X(n.top),bottom:X(n.bottom),right:X(n.right)},c='bottom'===o?'top':'bottom',u='right'===i?'left':'right',b=W("transform");if(d='bottom'===c?-f.height+h.bot tom:h.top,s='right'===u?-f.w
2022-07-01 14:30:01 UTC	327	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49828	104.18.10.207	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	257	OUT	GET /bootstrap/4.1.3/js/bootstrap.min.js HTTP/1.1 Host: stackpath.bootstrapcdn.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: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Referer: https://eyecandy lashcompany.com/payment/frontend_paper_lantern/index.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	327	IN	HTTP/1.1 200 OK Date: Fri, 01 Jul 2022 14:30:01 GMT Content-Type: application/javascript; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding CDN-PullZone: 252412 CDN-Uid: b1941f61-b576-4f40-80de-5677acb38f74 CDN-RequestCountryCode: DE Access-Control-Allow-Origin: * Cache-Control: public, max-age=31919000 Last-Modified: Mon, 25 Jan 2021 22:04:06 GMT CDN-CachedAt: 11/15/2021 23:30:00 CDN-ProxyVer: 1.0 CDN-RequestPullCode: 200 CDN-RequestPullSuccess: True CDN-EdgeStorageId: 723 CDN-Status: 200 timing-allow-origin: * cross-origin-resource-policy: cross-origin X-Content-Type-Options: nosniff CDN-RequestId: a35b0179a28ed953258d0fb41376a09c CDN-Cache: HIT CF-Cache-Status: HIT Age: 10626680 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Server: cloudflare CF-RAY: 723fd65308699107-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-01 14:30:01 UTC	328	IN	Data Raw: 31 30 61 66 0d 0a 2f 2a 21 0a 20 20 2a 20 42 6f 6f 74 73 74 72 61 70 20 76 34 2e 31 2e 33 20 28 68 74 74 70 73 3a 2f 2f 67 65 74 62 6f 6f 74 73 74 72 61 70 2e 63 6f 6d 2f 29 0a 20 20 2a 20 43 6f 70 79 72 69 67 68 74 20 32 30 31 31 2d 32 30 31 38 20 54 68 65 20 42 6f 6f 74 73 74 72 61 70 20 41 75 74 68 6f 72 73 20 28 68 74 74 70 73 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 74 77 62 73 2f 62 6f 6f 74 73 74 72 61 70 2f 67 72 61 70 68 73 2f 63 6f 6e 74 72 69 62 75 74 6f 72 73 29 0a 20 20 2a 20 4c 69 63 65 6e 73 65 64 20 75 6e 64 65 72 20 4d 49 54 20 28 68 74 74 70 73 3a 2f 2f 67 69 74 68 75 62 2e 63 6f 6d 2f 74 77 62 73 2f 62 6f 6f 74 73 74 72 61 70 2f 62 6c 6f 62 2f 6d 61 73 74 65 72 2f 4c 49 43 45 4e 53 45 29 0a 20 20 2a 2f 0a 21 66 75 6e 63 74 69 6f 6e 28 Data Ascii: 10af/*! * Bootstrap v4.1.3 (https://getbootstrap.com/) * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors) * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE) */function(
2022-07-01 14:30:01 UTC	328	IN	Data Raw: 71 75 69 72 65 28 22 70 6f 70 70 65 72 2e 6a 73 22 29 29 3a 22 66 75 6e 63 74 69 6f 6e 22 3d 3d 74 79 70 65 6f 66 20 64 65 66 69 6e 65 26 26 64 65 66 69 6e 65 2e 61 6d 64 3f 64 65 66 69 6e 65 28 5b 22 65 78 70 6f 72 74 73 22 2c 22 6a 71 75 65 72 79 22 2c 22 70 6f 70 70 65 72 2e 6a 73 22 5d 2c 65 29 3a 65 28 74 2e 62 6f 6f 74 73 74 72 61 70 3d 7b 7d 2c 74 2e 6a 51 75 65 72 79 2c 74 2e 50 6f 70 70 65 72 29 7d 28 74 68 69 73 2c 66 75 6e 63 74 69 6f 6e 28 74 2c 65 2c 68 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 69 28 74 2c 65 29 7b 66 6f 72 28 76 6 1 72 20 6e 3d 30 3b 6e 3c 65 2e 6c 65 6e 67 74 68 3b 6e 2b 2b 29 7b 76 61 72 20 69 3d 65 5b 6e 5d 3b 69 2e 65 6e 75 6d 65 72 61 62 6c 65 3d 69 2e 65 6e 75 6d 65 72 61 62 6c 65 7c 7c 21 Data Ascii: quire("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.boo tstrap={},t.jQuery,t.Popper)}(this,function(t,e,h){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerabl e=i.enumerable !
2022-07-01 14:30:01 UTC	329	IN	Data Raw: 2c 66 6e 2c 64 6e 2c 67 6e 2c 5f 6e 2c 6d 6e 2c 70 6e 2c 76 6e 2c 79 6e 2c 45 6e 2c 43 6e 2c 54 6e 2c 62 6e 2c 53 6e 2c 49 6e 2c 41 6e 2c 44 6e 2c 77 6e 2c 4e 6e 2c 4f 6e 2c 6b 6e 2c 50 6e 2c 6a 6e 2c 48 6e 2c 4c 6e 2c 52 6e 2c 78 6e 2c 57 6e 2c 55 6e 2c 71 6e 2c 46 6e 3d 66 75 6e 63 74 69 6f 6e 28 69 29 7b 76 61 72 20 65 3d 22 74 72 61 6e 73 69 74 69 6f 6e 65 6e 64 22 3b 66 75 6e 63 74 69 6f 6e 20 74 28 74 29 7b 76 61 72 20 65 3d 74 68 69 73 2c 6e 3d 21 31 3b 72 65 74 75 72 6e 20 69 28 74 68 69 73 29 2e 6f 6e 65 28 6c 2e 54 52 41 4e 53 49 54 49 4f 4e 5f 45 4e 44 2c 66 75 6 e 63 74 69 6f 6e 28 29 7b 6e 3d 21 30 7d 29 2c 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 7c 7c 6c 2e 74 72 69 67 67 65 72 54 72 61 6e 73 69 74 69 6f 6e 45 6e Data Ascii: ,fn,dn,gn,_,mn,pn,vn,yn,En,Cn,Tn,bn,Sn,ln,An,Dn,wn,Nn,On,kn,Pn,jn,Hn,Ln,Rn,xn,Wn,Un,qn,Fn=function(i){var e="transitionend";function t(t){var e=this,n=1;return i(this).one(l.TRANSITION_END,function(){n=0}),setTimeou t(function(){n l.triggerTransitionEn
2022-07-01 14:30:01 UTC	331	IN	Data Raw: 64 6c 65 3a 66 75 6e 63 74 69 6f 6e 28 74 29 7b 69 66 28 69 28 74 2e 74 61 72 67 65 74 29 2e 69 73 28 74 68 69 73 29 29 72 65 74 75 72 6e 20 74 2e 68 61 6e 64 6c 65 4f 62 6a 2e 68 61 6e 64 6c 65 72 2e 61 70 70 6c 79 28 74 68 69 73 2c 61 72 67 75 6d 65 6e 74 73 29 7d 7d 2c 6c 7d 28 65 29 2c 4b 6e 3d 28 6e 3d 22 61 6c 65 72 74 22 2c 61 3d 22 2e 22 2b 28 6f 3d 22 62 73 2e 61 6c 65 72 74 22 29 2c 63 3d 28 72 3d 65 29 2e 66 6e 5b 6e 5d 2c 75 3d 7b 43 4c 4f 53 45 3a 22 63 6c 6f 73 65 22 2b 61 2c 43 4c 4f 53 45 44 3a 22 63 6c 6f 73 65 64 22 2b 61 2c 43 4c 49 43 4b 5f 44 41 54 41 5f 41 50 49 3a 22 63 6c 69 63 6b 22 2b 61 2b 22 2e 64 61 74 61 2d 61 70 69 22 7d 2c 66 3d 22 61 6c 65 72 74 22 2c 64 3d 22 66 61 64 65 22 2c 67 3d 22 73 68 6f 77 22 2c 5f 3d 66 75 6e 63 Data Ascii: die:function(t){if(!t.target).is(this))return t.handleObj.handler.apply(this,arguments)}},l)(e),Kn=(n="alert",a="."+o="bs.alert"),c=(r=e).fn[n],u={CLOSE:"close"+a,CLOSED:"closed"+a,CLICK_DATA_API:"click"+a+"data-api"},f="aler t",d="fade",g="show",_="func
2022-07-01 14:30:01 UTC	332	IN	Data Raw: 37 66 66 61 0d 0a 22 63 6c 6f 73 65 22 3d 3d 3d 6e 26 26 65 5b 6e 5d 28 74 68 69 73 29 7d 29 7d 2c 69 2e 5f 68 61 6e 64 6c 65 44 69 73 6d 69 73 73 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 74 29 7b 74 26 26 74 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 2c 65 2e 63 6c 6f 73 65 28 74 68 69 73 29 7d 7d 2c 73 28 69 2c 6e 75 6c 6c 2c 5b 7b 6b 65 79 3a 22 56 45 52 53 49 4f 4e 22 2c 67 65 74 3a 66 75 6e 63 74 6 9 6f 6e 28 29 7b 72 65 74 75 72 6e 22 34 2e 31 2e 33 22 7d 7d 5d 29 2c 69 7d 28 29 2c 72 28 64 6f 63 75 6d 65 6e 74 29 2e 6f 6e 28 75 2e 43 4c 49 43 4b 5f 44 41 54 41 5f 41 50 49 2c 27 5b 64 61 74 61 2d 64 69 73 6d 69 73 73 3d 22 61 6c 65 72 74 22 5d 27 2c 5f 2e 5f 68 61 6e 64 6c 65 44 69 73 6d 69 73 73 Data Ascii: 7ffa"close"===n&&e[n](this)}},i._handleDismiss=function(e){return function(t){t&&t.preventDefault(),e.close (this)}},s(i,null,{key:"VERSION",get:function(){return"4.1.3"}}),t(),r(document).on(u.CLICK_DATA_API,{data-dismiss=" alert"},_._handleDismiss

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	333	IN	Data Raw: 49 6e 74 65 72 66 61 63 65 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 3d 6d 28 74 68 69 73 29 2e 64 61 74 61 28 76 29 3b 74 7c 7c 28 74 3d 6e 65 77 20 6e 28 74 68 69 73 29 2c 6d 28 74 68 69 73 29 2e 64 61 74 61 28 76 2c 74 29 29 2c 22 74 6f 67 6 7 6c 65 22 3d 3d 3d 65 26 26 74 5b 65 5d 28 29 7d 29 7d 2c 73 28 6e 2c 6e 75 6c 6c 2c 5b 7b 6b 65 79 3a 22 56 45 52 53 49 4f 4e 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 28 29 7b 72 65 74 75 72 6e 28 29 2c 6e 7d 28 29 2c 6d 28 64 6f 63 75 6d 65 6e 74 29 2e 6f 6e 28 4f 2e 43 4c 49 43 4b 5f 44 41 54 41 5f 41 50 49 2c 49 2c 66 75 6e 63 74 69 6f 6e 28 74 29 7b 74 2e 70 72 65 76 65 6e 74 44 65 66 61 Data Ascii: Interface=function(e){return this.each(function(){var t=m(this).data(v);t (t=new n(this),m(this).data(v,t)) ,"toggle"===e&&t[e]()}}),s(n,null,{key:"VERSION",get:function(){return"4.1.3"}}),n}),m(document).on(O.CLICK _DATA_API,l,function(t){t.preventDefault
2022-07-01 14:30:01 UTC	335	IN	Data Raw: 75 73 65 6c 22 5d 27 2c 6f 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 6f 28 74 2c 65 29 7b 74 68 69 73 2e 5f 69 74 65 6d 73 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 69 6e 74 65 72 76 61 6c 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 61 63 74 69 76 65 45 6c 65 6d 65 6e 74 3d 6e 75 6c 6c 74 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 69 73 53 6c 69 64 69 6e 67 3d 21 31 2c 74 68 69 73 2e 74 6f 75 63 68 54 69 6d 65 6f 75 74 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 63 6f 6e 66 69 67 3d 74 68 69 73 2e 5f 67 65 74 43 6f 6e 66 69 67 28 65 29 2c 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 3d 50 28 74 29 5b 30 5d 2c 74 68 69 73 2e 5f 69 6e 64 69 63 61 74 6f 72 73 45 6c 65 6d 65 6e 74 3d 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 2e 71 75 65 Data Ascii: user"]",ot=function(){function o(t,e){this._items=null,this._interval=null,this._activeElement=null,this._is Paused=!1,this._isSliding=!1,this.touchTimeout=null,this._config=this._getConfig(e),this._element=P(t)[0],this._indicato rsElement=this._element.que
2022-07-01 14:30:01 UTC	336	IN	Data Raw: 28 29 7b 50 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 6f 66 66 28 4c 29 2c 50 2e 72 65 6d 6f 76 65 44 61 74 61 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 2c 48 29 2c 74 68 69 73 2e 5f 69 74 65 6d 73 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 63 6f 6e 66 69 67 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 69 6e 74 65 72 76 61 6c 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 69 73 53 6c 69 64 69 6e 67 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 69 73 50 61 75 73 65 64 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 69 73 53 6c 69 64 69 6e 67 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 69 73 2e 5f 69 6e 64 69 63 61 74 6f 72 73 45 6c 65 6d 65 6e 74 3d 6e 75 6c 6c 7d 2c 74 2e 5f 67 65 74 43 6f 6e 66 69 67 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 Data Ascii: ()P(this._element).off(L),P.removeData(this._element,H),this._items=null,this._config=null,this._element=nu ll,this._interval=null,this._isPaused=null,this._isSliding=null,this._activeElement=null,this._indicatorsElement=null,t ._getConfig=function(t){ret
2022-07-01 14:30:01 UTC	337	IN	Data Raw: 2c 74 2e 5f 74 72 69 67 67 65 72 53 6c 69 64 65 45 76 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 74 2c 65 29 7b 76 61 72 20 6e 3d 74 68 69 73 2e 5f 67 65 74 49 74 65 6d 49 6e 64 65 78 28 74 29 2c 69 3d 74 68 69 73 2e 5f 67 65 74 49 74 65 6d 49 6e 64 65 78 28 74 29 2c 69 3d 74 68 69 73 2e 5f 67 65 74 29 29 2c 72 3d 50 2e 45 76 65 6e 74 28 51 2e 53 4c 49 44 45 2c 7b 72 65 6c 61 74 65 64 51 72 67 65 74 3a 74 2c 64 69 72 65 63 74 69 6f 6e 3a 65 2c 66 72 6f 6d 3a 69 2c 74 6f 3a 6e 7d 29 3b 72 65 74 75 72 6e 20 50 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 74 72 69 67 67 65 72 28 72 29 2c 72 7d 2c 74 2e 5f 73 65 74 41 63 74 69 76 65 49 6e 64 69 63 61 74 6f 72 45 6c 65 6d 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 74 Data Ascii: ,t._triggerSlideEvent=function(t,e){var n=this._getItemIndex(t),i=this._getItemIndex(this._element.querySele ctor(X)),r=P.Event(Q.SLIDE,{relatedTarget:t,direction:e,from:i,to:n});return P(this._element).trigger(r),r,t._setActive IndicatorElement=function(t
2022-07-01 14:30:01 UTC	339	IN	Data Raw: 7d 7d 2c 6f 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 3d 66 75 6e 63 74 69 6f 6e 28 69 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 3d 50 28 74 68 69 73 29 2e 64 61 74 61 28 48 29 2c 65 3d 6c 28 7b 7d 2c 57 2c 50 28 74 68 69 73 29 2e 64 61 74 61 28 29 29 3b 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 69 26 26 28 65 3d 6c 28 7b 7d 2c 65 2c 69 29 29 3b 76 61 72 20 6e 3d 22 73 74 72 6 9 6e 67 22 3d 3d 74 79 70 65 6f 66 20 69 3f 69 3a 65 2e 73 6c 69 64 65 3b 69 66 28 74 7c 7c 28 74 3d 6e 65 77 20 6f 28 74 68 69 73 2c 65 29 2c 50 28 74 68 69 73 29 2e 64 61 74 61 28 48 2c 74 29 29 2c 22 6e 75 6d 62 65 72 22 3d 3d 74 79 70 65 6f 66 20 69 29 74 2e 74 6f 28 69 29 3b 65 6c 73 65 20 69 66 28 Data Ascii: },o._jQueryInterface=function(i){return this.each(function(){var t=P(this).data(H),e=!({},W,P(this).data()) ;"object"!==typeof i&&(e=!({},e,i));var n="string"!==typeof i?i:e.slide;if(t (t=new o(this,e),P(this).data(H,t)),"number"!==typeof i)t.o(i);else if(
2022-07-01 14:30:01 UTC	340	IN	Data Raw: 69 63 6b 22 2b 63 74 2b 22 2e 64 61 74 61 2d 61 70 69 22 7d 2c 67 74 3d 22 73 68 6f 77 22 2c 5f 74 3d 22 63 6f 6c 6c 61 70 73 65 22 2c 6d 74 3d 22 63 6f 6c 6c 61 70 73 69 6e 67 22 2c 70 74 3d 22 63 6f 6c 6c 61 70 73 65 64 22 2c 76 74 3d 22 77 69 64 74 68 22 2c 79 74 3d 22 68 65 69 67 68 74 22 2c 45 74 3d 22 2e 73 68 6f 77 2c 20 2e 63 6f 6c 6c 61 70 73 69 6e 67 22 2c 43 74 3d 27 5b 64 61 74 61 2d 74 6f 67 67 6c 65 3d 22 63 6f 6c 6c 61 70 73 65 22 5d 27 2c 54 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 61 28 65 2c 74 29 7b 74 68 69 73 2e 5f 69 73 54 72 6 1 6e 73 69 74 69 6f 6e 69 6e 67 3d 21 31 2c 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 3d 65 2c 74 68 69 73 2e 5f 63 6f 6e 6 6 69 67 3d 74 68 69 73 2e 5f 67 65 74 43 6f 6e 66 69 67 28 74 29 Data Ascii: ick"+ct+",.data-api"),gt="show",_t="collapse",mt="collapsing",pt="collapsed",vt="width",yt="height",Et=".show, .collapsing",Ct="[data-toggle='collapse']",Tt=function(){function a(e,t){this._isTransitioning=!1,this._element=e,this ._config=this._getConfig(t)
2022-07-01 14:30:01 UTC	341	IN	Data Raw: 61 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 2e 63 61 6c 6c 28 73 74 28 74 29 2e 6e 6f 74 28 74 68 69 73 2e 5f 73 65 6c 65 63 74 6f 72 29 2c 22 68 69 64 65 22 29 2c 65 7c 7c 73 74 28 74 29 2e 64 61 74 61 28 6c 74 2c 6e 75 6c 6c 29 29 3b 76 61 72 20 72 3d 74 68 69 73 2e 5f 67 65 74 44 69 6d 65 6e 73 69 6f 6e 28 29 3b 73 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 5f 74 29 2e 61 64 64 43 6c 61 73 73 28 6d 74 29 2c 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 2e 73 74 79 6c 65 5b 72 5d 3d 30 2c 74 68 69 73 2e 5f 74 72 69 67 67 65 72 41 72 72 61 79 2e 6c 65 6e 67 74 68 26 26 73 74 28 74 68 69 73 2e 5f 67 69 67 67 65 72 41 72 72 61 79 29 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 70 74 29 2e 61 74 74 72 28 22 61 72 Data Ascii: a._jQueryInterface.call(st(t),not(this._selector),"hide"),e st(t).data(t,null));var r=this._getDimension();st(this._ element).removeClass(_t).addClass(mt),this._element.style[r]=0,this._triggerArray.length&&st(this._triggerArray).removeC lass(pt).attr("ar
2022-07-01 14:30:01 UTC	343	IN	Data Raw: 65 6d 65 6e 74 29 2e 6f 6e 65 28 46 6e 2e 54 52 41 4e 53 49 54 49 4f 4e 5f 45 4e 44 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 74 2e 73 65 74 54 72 61 6e 73 69 74 69 6f 6e 69 6e 67 28 21 31 29 2c 73 74 28 74 2e 5f 65 6c 65 6d 65 6e 74 29 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 6d 74 29 2e 61 64 64 43 6c 61 73 73 28 5f 74 29 2e 74 72 69 67 67 65 72 28 64 74 2e 48 49 44 44 45 4e 29 7d 29 2e 65 6d 75 6c 61 74 65 54 72 61 6e 73 69 74 69 6f 6e 69 6e 67 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 74 68 69 73 2e 5f 69 73 54 72 61 6e 73 69 74 69 6f 6e 69 6e 67 3d 74 7d 2c 74 2e 64 69 73 70 6f 73 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 73 74 2e 72 65 6d 6f 76 65 44 61 74 61 28 74 68 69 73 2e 5f 65 6c 65 Data Ascii: ement).one(Fn.TRANSITION_END,function(){t.setTransitioning(!1),st(t._element).removeClass(mt).addC lass(_t).trigger(dt.HIDDEN)}).emulateTransitionEnd(a)}}),t.setTransitioning=function(t){this._isTransitioning=t,t.dispo se=function(){st.removeData(this,_ele

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	344	IN	Data Raw: 26 26 2f 73 68 6f 77 7c 68 69 64 65 2f 2e 74 65 73 74 28 69 29 26 26 28 6e 2e 74 6f 67 67 6c 65 3d 21 31 29 2c 65 7c 7c 28 65 3d 6e 65 77 20 61 28 74 68 69 73 2c 6e 29 2c 74 2e 64 61 74 61 28 6c 74 2c 65 29 29 2c 22 73 74 72 69 6e 67 22 3d 3d 74 79 70 65 6f 66 20 69 29 7b 69 66 28 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f 66 20 65 5b 69 5d 29 74 68 72 6f 77 20 6e 65 77 20 54 79 70 65 45 72 72 6f 72 28 27 4e 6f 20 6d 65 74 68 6f 64 20 6e 61 6d 65 64 20 22 27 2b 69 2b 27 22 27 29 3b 65 5b 69 6d 28 29 7d 7d 29 7d 2c 73 28 61 2c 7b 6b 65 79 3d 22 56 45 52 53 49 4f 4e 22 2c 67 65 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 22 34 2e 31 2e 33 22 7d 7d 2c 7b 6b 65 79 3a 22 44 65 66 61 75 6c 74 22 2c 67 65 74 3a 66 75 6e Data Ascii: &&#x27;test(i)&&(n.toggle=1),e (e=new a(this,n),t.data(lt,e)),"string"==typeof i){if("undefined"==typeof e[i])throw new TypeError("No method named '"+i+"'");e[i]()}}},s(a,null,{key:"VERSION",get:function(){return"4.1.3"}},{key:"Default",get:fun
2022-07-01 14:30:01 UTC	345	IN	Data Raw: 2c 62 6f 75 6e 64 61 72 79 3a 22 73 63 72 6f 6c 6c 50 61 72 65 6e 74 22 2c 72 65 66 65 72 65 6e 63 65 3a 22 74 6f 67 67 6c 65 22 2c 64 69 73 70 6c 61 79 3a 22 64 79 6e 61 6d 69 63 22 7d 2c 5a 74 3d 7b 6f 66 66 73 65 74 3a 22 28 6e 75 6d 62 65 72 7c 73 74 72 69 6e 67 7c 66 75 6e 63 74 69 6f 6e 29 22 2c 66 6c 69 70 3a 22 62 6f 6f 6c 65 61 6e 22 2c 62 6f 75 6e 64 61 72 79 3a 22 28 73 74 72 69 6e 67 7c 65 6c 65 6d 65 6e 74 29 22 2c 72 65 66 65 72 65 6e 63 65 3a 22 28 73 74 72 69 6e 67 7c 65 6c 65 6d 65 6e 74 29 22 2c 64 69 73 70 6c 61 79 3a 22 73 74 72 69 6e 67 22 7d 2c 47 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 63 28 74 2c 65 29 7b 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 3d 74 2c 74 68 69 73 2e 5f 70 6f 70 70 65 72 3d 6e 75 6c 6c 2c Data Ascii: ,boundary:"scrollParent",reference:"toggle",display:"dynamic"),Zt={offset:(number string function)",flip:"boolean",boundary:"(string element)",reference:"(string element)",display:"string"),Gt=function(){function c(t,e){this._element=t,this._popper=null,
2022-07-01 14:30:01 UTC	347	IN	Data Raw: 2c 62 74 28 74 29 2e 74 6f 67 67 6c 65 43 6c 61 73 73 28 50 74 29 2e 74 72 69 67 67 65 72 28 62 74 2e 45 76 65 6e 74 28 4f 74 2e 53 48 4f 57 4e 2c 6e 29 29 7d 7d 7d 2c 74 2e 64 69 73 70 6f 73 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 62 74 2e 72 65 6d 6f 76 65 44 61 74 61 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 2c 49 74 29 2c 62 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 6f 66 66 28 41 74 29 2c 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 3d 6e 75 6c 6c 2c 28 74 68 69 73 2e 5f 6d 65 6e 75 3d 6e 75 6c 6c 29 21 3d 3d 74 68 69 73 2e 5f 70 6f 70 70 65 72 3d 6e 75 6c 6c 29 7d 2c 74 2e 75 70 64 61 74 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 68 Data Ascii: ,bt(t).toggleClass(Pt).trigger(bt.Event(Ot.SHOWN,n))}}}},t.dispose=function(){bt.removeData(this._element,lt),bt(this._element).off(At),this._element=null,(this._menu=null)!=this._popper&&(this._popper.destroy(),this._popper=null),t.update=function(){th
2022-07-01 14:30:01 UTC	348	IN	Data Raw: 77 3a 7b 62 6f 75 6e 64 61 72 69 65 73 45 6c 65 6d 65 6e 74 3a 74 68 69 73 2e 5f 63 6f 6e 66 69 67 2e 62 6f 75 6e 64 61 72 79 7d 7d 7d 3b 72 65 74 75 72 6e 22 73 74 61 74 69 63 22 3d 3d 3d 74 68 69 73 2e 5f 63 6f 6e 66 69 67 2e 64 69 73 70 6c 61 79 26 26 28 6e 2e 6d 6f 64 69 66 69 65 72 73 2e 61 70 6c 79 53 74 79 6c 65 3d 7b 65 6e 61 62 6c 65 64 3a 21 31 7d 29 2c 6e 7d 2c 63 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 3d 66 75 6e 63 74 69 6f 6e 2 8 65 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 65 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 3d 62 74 28 74 68 69 73 29 2e 64 61 74 61 28 49 74 29 3b 69 66 28 74 7c 7c 28 74 3d 6e 65 77 20 63 28 74 68 69 73 2c 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 65 3f 65 3a 6e 75 6c 6c 29 Data Ascii: w:{boundariesElement:this._config.boundary}}};return"static"===this._config.display&&(n.modifiers.applyStyle={enabled:1!}),n,c._jQueryInterface=function(e){return this.each(function(){var t=bt(this).data(lt);if(!t (t=new c(this,"object"==>typeof e?e:null)
2022-07-01 14:30:01 UTC	349	IN	Data Raw: 69 63 68 26 26 33 38 21 3d 3d 74 2e 77 68 69 63 68 7c 7c 62 74 28 74 2e 74 61 72 67 65 74 29 2e 63 6c 6f 73 65 73 74 28 71 74 29 2e 6c 65 6e 67 74 68 29 29 3a 4e 74 2e 74 65 73 74 28 74 2e 77 68 69 63 68 29 29 26 26 28 74 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 2c 74 2e 73 74 6f 70 50 72 6f 70 61 67 61 74 69 6f 6e 28 29 2c 21 74 68 69 73 2e 64 69 73 61 62 6c 65 64 26 26 21 62 74 28 74 68 69 73 29 2e 68 61 73 43 6c 61 73 73 28 6b 74 29 29 29 7b 76 61 72 20 65 3d 63 2e 5f 67 65 74 50 61 72 65 6e 74 46 72 6f 6d 45 6c 65 6d 65 6e 74 28 74 68 69 73 29 2c 6e 3d 62 74 2 8 65 29 2e 68 61 73 43 6c 61 73 73 28 50 74 29 3b 69 66 28 28 6e 7c 7c 32 37 3d 3d 3d 74 2e 77 68 69 63 68 26 26 33 32 3d 3d 3d 74 2e 77 68 69 63 68 29 26 26 28 21 6e 7c 7c 32 37 21 3d Data Ascii: ich&&#38;!=t.which bt(t.target).closest(qt).length)):Nt.test(t.which))&&(t.preventDefault(),t.stopPropagation n(),!this.disabled&&!bt(this).hasClass(kt)){var e=c._getParentFromElement(this),n=bt(e).hasClass(Pt);if((n t===t.whic h&&#32;==t.which)&&(!n 27!=
2022-07-01 14:30:01 UTC	351	IN	Data Raw: 7d 2c 6f 65 3d 7b 48 49 44 45 3a 22 68 69 64 65 22 2b 65 65 2c 48 49 44 44 45 4e 3a 22 68 69 64 64 65 6e 22 2b 65 65 2c 53 48 4f 57 3a 22 73 68 6f 77 22 2b 65 65 2c 53 48 4f 57 4e 3a 22 73 68 6f 77 6e 22 2b 65 65 2c 46 4f 43 55 53 49 4e 3a 22 66 6f 63 75 73 69 6e 22 2b 65 65 2c 52 45 53 49 5a 45 3a 22 72 65 73 69 7a 65 22 2b 65 65 2c 43 4c 49 43 4b 5f 44 49 53 4d 49 53 53 3a 22 63 6c 69 63 6b 2e 64 69 73 6d 69 73 73 22 2b 65 65 2c 4b 45 59 44 4f 57 4e 5f 44 49 53 4d 49 53 53 3a 22 6b 65 79 64 6f 77 6e 2e 64 69 73 6d 69 73 73 22 2b 65 65 2c 4d 4f 55 53 45 55 50 5f 44 49 53 4d 49 53 53 3a 22 6d 6f 75 73 65 75 70 2e 64 69 73 6d 69 73 73 22 2b 65 65 2c 4d 4f 55 53 45 44 4f 57 4e 5f 44 49 53 4d 49 53 53 3a 22 6f 75 73 65 64 6f 77 6e 2e 64 69 73 6d 69 73 73 Data Ascii: },oe=[HIDE:"hide"+ee,HIDDEN:"hidden"+ee,SHOW:"show"+ee,SHOWN:"shown"+ee,FOCUSIN:"focusin "+ee,RESIZE:"resize"+ee,CLICK_DISMISS:"click.dismiss"+ee,KEYDOWN_DISMISS:"keydown.dismiss"+ee,MOUSEUP_P_DISMISS:"mouseup.dismiss"+ee,MOUSEDOWN_DISMISS:"mousedown.dismiss
2022-07-01 14:30:01 UTC	352	IN	Data Raw: 74 69 6f 6e 28 29 7b 24 74 28 65 2e 5f 65 6c 65 6d 65 6e 74 29 2e 6f 6e 65 28 6f 65 2e 4d 4f 55 53 45 55 50 5f 44 49 53 4d 49 53 53 2c 66 75 6e 63 74 69 6f 6e 28 74 29 7b 24 74 28 74 2e 74 61 72 67 65 74 29 2e 69 73 28 65 2e 5f 65 6c 65 6d 65 6e 74 29 26 26 28 65 2e 5f 69 67 6e 6f 72 65 42 61 63 6b 64 72 6f 70 28 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 65 2e 5f 73 68 6f 77 45 6c 65 6d 65 6e 74 28 74 29 7d 29 29 7d 7d 2c 74 2e 68 69 64 65 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 65 3d 74 68 69 73 3b 69 66 28 74 26 26 74 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 2c 21 74 68 69 73 2e 5f 69 73 54 72 61 6e 73 69 74 69 6f 6e 69 6e 67 Data Ascii: tion(){\$t(e._element).one(oe.MOUSEUP_DISMISS,function(t){\$t(t.target).is(e._element)&&(e._ignoreBackdropClick=!0)})),this._showBackdrop(function(){return e._showElement(t)})),t.hide=function(t){var e=this;if(t&&t.pr eventDefault(),!this._isTransitioning
2022-07-01 14:30:01 UTC	353	IN	Data Raw: 65 2e 6e 6f 64 65 54 79 70 65 3d 3d 3d 4e 6f 64 65 2e 45 4c 45 4d 45 4e 54 5f 4e 4f 44 45 7c 7c 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2c 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 2e 73 74 79 6c 65 2e 64 69 73 70 6c 61 79 3d 22 62 6c 6f 63 6b 22 2c 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 2e 72 65 6d 6f 76 65 41 74 74 72 69 62 75 74 65 28 22 61 72 69 61 2d 68 69 64 64 65 6e 22 29 2c 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 2e 73 63 72 6f 6c 6c 54 6f 70 3d 30 2c 6e 26 26 46 6e 2e 72 65 66 6c 6f 77 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2c 24 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 61 64 64 43 6c 61 73 7 3 28 68 65 29 2c 74 68 69 73 2e 5f 63 6f 6e 66 69 67 2e 66 6f 63 Data Ascii: e.nodeType===Node.ELEMENT_NODE document.body.appendChild(this._element),this._element.style.display="block",this._element.removeAttribute("aria-hidden"),this._element.scrollTop=0,n&&Fn.reflow(this._element),\$(this._element).addClass(he),this._config.foc

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	355	IN	Data Raw: 65 74 53 63 72 6f 6c 6c 62 61 72 28 29 2c 24 74 28 74 2e 5f 65 6c 65 6d 65 6e 74 29 2e 74 72 69 67 67 65 72 28 6f 65 2e 48 49 44 44 45 4e 29 7d 29 7d 2c 74 2e 5f 72 65 6d 6f 76 65 42 61 63 6b 64 72 6f 70 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 68 69 73 2e 5f 62 61 63 6b 64 72 6f 70 26 26 28 24 74 28 74 68 69 73 2e 5f 62 61 63 6b 64 72 6f 70 29 2e 72 65 6d 6f 76 65 28 29 2c 74 68 69 73 2e 5f 62 61 63 6b 64 72 6f 70 3d 6e 75 6c 6c 29 7d 2c 74 2e 5f 73 68 6f 77 42 61 63 6b 64 72 6f 70 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 65 3d 74 68 69 73 2c 6e 3d 24 74 28 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 29 2e 68 61 73 43 6c 61 73 73 28 63 65 29 3f 63 65 3a 22 22 3b 69 66 28 74 68 69 73 2e 5f 69 73 53 68 6f 77 6e 26 26 74 68 69 73 2e 5f 63 6f 6e 66 69 67 Data Ascii: etScrollbar(),\$(t._element).trigger(oe.HIDDEN))),t._removeBackdrop=function(){this._backdrop&\$(t(this._backdrop).remove(),this._backdrop=null)),t._showBackdrop=function(t){var e=this,n=\$(this._element).hasClass(ce)?ce:"";if(this._isShown&&this._config
2022-07-01 14:30:01 UTC	356	IN	Data Raw: 61 64 64 69 6e 67 52 69 67 68 74 3d 74 68 69 73 2e 5f 73 63 72 6f 6c 6c 62 61 72 57 69 64 74 68 2b 22 70 78 22 29 7d 2c 74 2e 5f 72 65 73 65 74 41 64 6a 75 73 74 6d 65 6e 74 73 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 2e 73 74 79 6c 65 2e 70 61 64 64 69 6e 67 4c 65 66 74 3d 22 2c 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 2e 73 74 79 6c 65 2e 70 61 64 64 69 6e 67 52 69 67 68 74 3d 22 22 7d 2c 74 2e 5f 63 68 65 63 6b 53 63 72 6f 6c 6c 62 61 72 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 3d 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 2e 67 65 74 42 6f 75 6e 64 69 6e 67 43 6c 69 65 6e 74 52 65 63 74 28 29 3b 74 68 69 73 2e 5f 69 73 42 6f 64 79 4f 76 65 72 66 6c 6f 77 69 6e 67 3d 74 2e 6c 65 66 74 2b 74 2e 72 69 67 68 74 3c Data Ascii: addingRight=this._scrollbarWidth+"px")),t._resetAdjustments=function(){this._element.style.paddingLeft="",this._element.style.paddingRight=""},t._checkScrollbar=function(){var t=document.body.getBoundingClientRect();this._isBodyOverflowing=t.left+t.right<
2022-07-01 14:30:01 UTC	357	IN	Data Raw: 2c 6e 29 2e 72 65 6d 6f 76 65 44 61 74 61 28 22 6d 61 72 67 69 6e 2d 72 69 67 68 74 22 29 7d 29 3b 76 61 72 20 6e 3d 24 74 28 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 29 2e 64 61 74 61 28 22 70 61 64 64 69 6e 67 2d 72 69 67 68 74 22 29 3b 24 74 28 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 29 2e 72 65 6d 6f 76 65 44 61 74 61 28 22 70 61 64 64 6 9 6e 67 2d 72 69 67 68 74 22 29 2c 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 2e 73 74 79 6c 65 2e 70 61 64 64 69 6e 67 52 69 67 68 74 3d 6e 7c 7c 22 22 7d 2c 74 2e 5f 67 65 74 53 63 72 6f 6c 62 61 72 57 69 64 74 68 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 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 64 69 76 22 29 3b 74 2e 63 6c 61 73 73 4e 61 6d 65 3d 73 65 2c 64 6f 63 75 6d 65 6e Data Ascii: ,n).removeData("margin-right"));var n=\$(document.body).data("padding-right");\$(document.body).removeData("padding-right"),document.body.style.paddingRight=n "",t._getScrollbarWidth=function(){var t=document.createElement("div");t.className=se,documen
2022-07-01 14:30:01 UTC	359	IN	Data Raw: 74 6f 6f 6c 74 69 70 22 29 2c 43 65 3d 28 70 65 3d 65 29 2e 66 6e 5b 76 65 5d 2c 54 65 3d 22 62 73 2d 74 6f 6f 6c 74 69 70 22 2c 62 65 3d 6e 65 77 20 52 65 67 45 78 70 28 22 28 5e 7c 5c 5c 73 29 22 2b 54 65 2b 22 5c 5c 53 2b 22 2c 22 67 22 29 2c 41 65 3d 7b 61 6e 69 6d 61 74 69 6f 6e 3a 21 30 2c 74 65 6d 70 6c 61 74 65 3a 27 3c 64 69 76 20 63 6c 61 73 73 3d 22 74 6f 6f 6c 74 69 70 22 20 72 6f 6c 65 3d 22 74 6f 6f 6c 74 69 70 22 3c 6c 64 69 76 20 63 6c 61 73 73 3d 22 61 72 72 6f 77 22 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 74 6f 6f 6c 74 69 70 2d 69 6e 6e 65 72 22 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 27 2c 74 72 69 67 67 65 72 3a 22 68 6f 76 65 72 20 66 6f 63 75 73 22 2c 74 69 74 6c 65 3a 22 22 2c 64 65 6c 61 79 3a 30 2c 68 74 6d 6c 3a Data Ascii: tooltip"),Ce=(pe=e).fn[ve],Te="bs-tooltip",be=new RegExp("(^ \\s)"+"Te+"\\s+", "g"),Ae={animation:!0,template:'<div class="tooltip" role="tooltip"><div class="arrow"></div><div class="tooltip-inner"></div></div>',trigger:"hover focus",title:"",delay:0,html:
2022-07-01 14:30:01 UTC	360	IN	Data Raw: 73 74 65 6e 65 72 73 28 29 7d 76 61 72 20 74 3d 69 2e 70 72 6f 74 6f 74 79 70 65 3b 72 65 74 75 72 6e 20 74 2e 65 6e 61 62 6c 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 68 69 73 2e 5f 69 73 45 6e 61 62 6c 65 64 3d 21 30 7d 2c 74 2e 64 69 73 61 62 6c 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 68 69 73 2e 5f 69 73 45 6e 61 62 6c 65 64 3d 21 31 7d 2c 74 2e 74 6f 67 67 6c 65 45 6e 61 62 6c 65 64 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 68 69 73 2e 5f 69 73 45 6e 61 62 6c 65 64 3d 21 74 68 69 73 2e 5f 69 73 45 6e 61 62 6c 65 64 7d 2c 74 2e 74 6f 67 67 6c 65 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 69 66 28 74 68 69 73 2e 5f 69 73 45 6e 61 62 6c 65 64 29 69 66 28 74 29 7b 76 61 72 20 65 3d 74 68 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 44 41 54 41 5f 4b 45 59 2c Data Ascii: steners()}}var t=i.prototype;return t.enable=function(){this._isEnabled=!0},t.disable=function(){this._isEnabled=!1},t.toggleEnabled=function(){this._isEnabled=!this._isEnabled},t.toggle=function(t){if(this._isEnabled){if(t){var e=this.constructor.DATA_KEY,
2022-07-01 14:30:01 UTC	361	IN	Data Raw: 65 6e 74 65 64 28 29 7c 7c 21 6e 29 72 65 74 75 72 6e 3b 76 61 72 20 69 3d 74 68 69 73 2e 67 65 74 54 69 70 45 6c 65 6d 65 6e 74 28 29 2c 72 3d 46 6e 2e 67 65 74 55 49 44 28 74 68 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 4e 41 4d 45 29 3b 69 2e 73 65 74 41 74 74 72 69 62 75 74 65 28 22 69 64 22 2c 72 29 2c 74 68 69 73 2e 65 6c 65 6d 65 6e 74 2e 73 65 74 41 74 74 72 69 62 75 74 65 28 22 61 72 69 61 2d 64 65 73 63 72 69 62 65 64 62 79 22 2c 72 29 2c 74 68 69 73 2e 73 65 74 43 6f 6e 74 65 6e 74 28 29 2c 74 68 69 73 2e 63 6f 6e 66 69 67 2e 61 6e 69 6d 61 74 69 6f 6e 26 26 70 65 28 69 29 2e 61 64 64 43 6c 61 73 73 28 4f 65 29 3b 76 61 72 20 6f 3d 22 66 75 6e 63 74 69 6f 6e 22 3d 3d 74 79 70 65 6f 66 20 74 68 69 73 2e 63 6f 6e 66 69 67 2e 70 6c 61 63 65 6d Data Ascii: ented() !n)return;var i=this.getTipElement(),r=Fn.getUID(this.constructor.NAME);i.setAttribute("id",r),this.element.setAttribute("aria-describedby",r),this.setContent(),this.config.animation&&pe(i).addClass(Oe);var o="function"==typeof this.config.placem
2022-07-01 14:30:01 UTC	363	IN	Data Raw: 46 72 6f 6d 45 6c 65 6d 65 6e 74 28 74 68 69 73 2e 74 69 70 29 3b 70 65 74 68 69 73 2e 74 69 70 29 2e 6f 6e 65 28 46 6e 2e 54 52 41 4e 53 49 54 49 4f 4e 5f 45 4e 44 2c 6c 29 2e 65 6d 75 6c 61 74 65 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 63 29 7d 65 6c 73 65 20 6c 28 29 7d 7d 2c 74 2e 68 69 64 65 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 76 61 72 20 65 3d 74 68 69 73 2c 6e 3d 74 68 69 73 2e 67 65 74 54 69 70 45 6c 65 6d 65 6e 74 28 29 2c 69 3d 70 65 2e 45 76 65 6e 74 28 74 68 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 45 76 65 6e 74 2e 48 49 44 45 29 2c 72 3d 66 75 6e 6 3 74 69 6f 6e 28 29 7b 65 2e 5f 68 6f 76 65 72 53 74 61 74 65 21 3d 3d 44 65 26 26 6e 2e 70 61 72 65 6e 74 4e 6f 64 65 26 26 6e 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 72 65 6d 6f 76 65 43 Data Ascii: FromElement(this.tip);pe(this.tip).one(Fn.TRANSITION_END,l).emulateTransitionEnd(c))else l()}}t.hide=function(t){var e=this,n=this.getTipElement(),i=pe.Event(this.constructor.Event.HIDE),r=function(){e._hoverState!=De&&n.parentNode&&n.parentNode.removeChild
2022-07-01 14:30:01 UTC	364	IN	Data Raw: 33 36 62 36 0d 0a 73 28 4f 65 2b 22 20 22 2b 6b 65 29 7d 2c 74 2e 73 65 74 45 6c 65 6d 65 6e 74 43 6f 6e 74 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 74 2c 65 29 7b 76 61 72 20 6e 3d 74 68 69 73 2e 63 6f 6e 66 69 67 2e 68 74 6d 6c 3b 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 65 26 26 28 65 2e 6e 6f 64 65 54 79 70 65 7c 7c 65 2e 6a 71 75 65 72 79 29 3f 6e 3f 70 65 28 65 29 2e 70 61 72 65 6e 74 28 29 2e 69 73 28 74 29 7c 7c 74 2e 65 6d 70 74 79 28 29 2e 61 70 70 65 6e 64 28 65 29 3a 74 2e 74 65 78 74 28 70 65 28 65 29 2e 74 65 78 74 28 29 29 3a 74 5b 6e 3f 22 68 74 6d 6c 22 3a 22 74 65 78 74 22 5d 28 65 29 7d 2c 74 2e 67 65 74 54 69 74 6c 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 3d 74 68 69 73 2e 65 6c 65 6d 65 6e 74 2e 67 65 74 41 74 74 Data Ascii: 36b6s(Oe+" "+ke)),t.setElementContent=function(t,e){var n=this.config.html;"object"==typeof e&&(e.nodeType e.jquery)?n?pe(e).parent().is(t) t.empty().append(e):t.text(pe(e).text()):t[n?"html":"text"](e),t.getTitle=function(){var t=this._element.getAtt

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	365	IN	Data Raw: 74 6c 65 22 2c 22 22 29 29 7d 2c 74 2e 5f 65 6e 74 65 72 3d 66 75 6e 63 74 69 6f 6e 28 74 2c 65 29 7b 76 61 72 20 6e 3d 74 68 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 44 41 54 41 5f 4b 45 59 3b 28 65 3d 65 7c 7c 70 65 28 74 2e 63 75 72 72 65 6e 74 54 61 72 67 65 74 29 2e 64 61 74 61 28 6e 29 29 7c 7c 28 65 3d 6e 65 77 20 74 68 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 28 74 2e 63 75 72 72 65 6e 74 54 61 72 67 65 74 2c 74 68 69 73 2e 5f 67 65 74 44 65 6c 65 67 61 74 65 43 6f 6e 66 69 67 28 29 2c 70 65 28 74 2e 63 75 72 72 65 6e 74 54 61 72 67 65 74 2c 65 6f 6e 66 69 67 28 2e 64 61 74 61 28 6e 2c 65 29 2c 74 26 26 28 65 2e 5f 61 63 74 69 76 65 54 72 69 67 67 65 72 5b 22 66 6f 63 75 73 69 6e 22 3d 3d 3d 74 2e 74 79 70 65 3f 4c 65 3a 48 65 5d 3d 21 30 29 2c 70 65 28 65 Data Ascii: tle="",""));,t._enter=function(t,e){var n=this.constructor.DATA_KEY;(e=e pe(t.currentTarget).data(n)) (e=new this.constructor(t.currentTarget,this._getDelegateConfig()),pe(t.currentTarget).data(n,e)),t&&(e._activeTrigger["focusi n"]=="=t.type?Le:He"]=0),pe(e
2022-07-01 14:30:01 UTC	367	IN	Data Raw: 68 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 44 65 66 61 75 6c 74 54 79 70 65 29 2c 74 7d 2c 74 2e 5f 67 65 74 44 65 6c 65 67 61 74 65 43 6f 6e 66 69 67 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 3d 7b 7d 3b 69 66 28 74 68 69 73 2e 63 6f 6e 66 69 67 29 66 6f 72 28 76 61 72 20 65 20 69 6e 20 74 68 69 73 2e 63 6f 6e 66 69 67 29 74 68 69 73 2e 63 6f 6e 73 74 72 75 63 74 6f 72 2e 44 65 66 61 75 6c 74 5b 65 5d 21 3d 3d 74 68 69 73 2e 63 6f 6e 66 69 67 5b 65 5d 26 26 28 74 5b 65 5d 3d 74 68 69 73 2e 63 6f 6e 66 69 67 5b 65 5d 29 3b 72 65 74 75 72 6e 20 74 7d 2c 74 2e 5f 63 6c 65 61 6e 54 69 70 43 6c 61 73 73 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 74 3d 70 65 28 74 68 69 73 2e 67 65 74 54 69 70 45 6c 65 6d 65 6e 74 28 29 29 2c 65 3d 74 2e 61 Data Ascii: his.constructor.DefaultType),t),t._getDelegateConfig=function(){var t={};if(this.config)for(var e in this.config)this.constructor.Default[e]!==this.config[e]&&(t[e]=this.config[e]);return t},t._cleanTipClass=function(){var t=pe(this.getTipElement()),e=t.a
2022-07-01 14:30:01 UTC	368	IN	Data Raw: 2e 6e 6f 43 6f 6e 66 6c 69 63 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 70 65 2e 66 6e 5b 76 65 5d 3d 43 65 2c 57 65 2e 5f 6a 51 75 65 72 79 49 6e 74 65 72 66 61 63 65 7d 2c 57 65 29 2c 4a 6e 3d 28 71 65 3d 22 70 6f 70 6f 76 65 72 22 2c 4b 65 3d 22 2e 22 2b 28 46 65 3d 22 62 73 2e 70 6f 70 6f 76 65 72 22 2c 42 65 3d 6e 65 77 20 52 65 67 45 78 70 28 22 28 5e 7c 5c 5c 73 29 22 2b 51 65 2b 22 5c 5c 53 2b 22 2c 22 67 22 29 2c 56 65 3d 6c 28 7b 7d 2c 7a 6e 2e 4 4 65 66 61 75 6c 74 2c 7b 70 6c 61 63 65 6d 65 6e 74 3a 22 72 69 67 68 74 22 2c 74 72 69 67 67 65 72 3a 22 63 6c 69 63 6b 22 2c 63 6f 6e 74 65 6e 74 3a 22 22 2c 74 65 6d 70 6c 61 74 65 Data Ascii: .noConflict=function(){return pe.fn[ve]=Ce,We._jQueryInterface},We),Jn=(qe="popover",Ke="."+{Fe="b s.popover"},Me=(Ue=e).fn[qe],Qe="bs-popover",Be=new RegExp("(^ \\s)+Qe+\\s+","g")),Ve=(l({}),zn.Default,{placem ent:"right",trigger:"click",content:"",template
2022-07-01 14:30:01 UTC	369	IN	Data Raw: 73 73 28 7a 65 2b 22 20 22 2b 4a 65 29 7d 2c 72 2e 5f 67 65 74 43 6f 6e 74 65 6e 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 65 6c 65 6d 65 6e 74 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 64 61 74 61 2d 63 6f 6e 74 65 6e 74 22 29 7c 7c 74 68 69 73 2e 63 6f 6e 66 69 67 2e 63 6f 6e 74 65 6e 74 7d 2c 72 2e 5f 63 6c 65 61 6e 54 69 70 43 6c 61 73 73 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 3d 55 65 28 74 68 69 73 2e 67 65 74 54 69 70 45 6c 65 6d 65 6e 74 28 29 29 2c 65 3d 74 2e 61 74 74 72 28 22 63 6c 61 73 73 22 29 2e 6d 61 74 63 68 28 42 65 29 3b 6e 75 6c 6c 21 3d 3d 65 26 26 30 3c 65 2e 6c 65 6e 74 67 68 26 26 74 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 65 2e 6a 6f 69 6e 28 22 22 29 29 7d 2c 69 2e 5f 6a 51 75 65 72 Data Ascii: ss(ze+" "+Je)),r._getContent=function(){return this.element.getAttribute("data-content")} this.config.conten t},r._cleanTipClass=function(){var t=Ue(this.getTipElement()),e=t.attr("class").match(Be);null!==(e&&e.length&&t.remove Class(e.join(""))),i._jQuery
2022-07-01 14:30:01 UTC	371	IN	Data Raw: 74 2d 67 72 6f 75 70 2d 69 74 65 6d 22 2c 70 6e 3d 22 2e 64 72 6f 70 64 6f 77 6e 22 2c 76 6e 3d 22 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6e 65 22 2c 45 6e 3d 22 6f 66 66 73 65 74 22 2c 43 6e 3d 22 70 6f 73 69 74 69 6f 6e 22 2c 54 6e 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 6e 28 74 2c 65 29 7b 76 61 72 20 6e 3d 74 68 69 73 3b 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 3d 74 2c 74 68 69 73 2e 5f 73 63 72 6f 6c 6c 45 6c 65 6d 65 6e 74 3d 22 42 4f 44 59 22 3d 3d 3d 74 2e 74 61 67 4e 61 6d 65 3f 77 69 6e 64 6f 77 3a 74 2c 74 68 69 73 2e 5f 63 6f 6e 66 69 67 3d 74 68 69 73 2e 5f 67 65 74 43 6f 6e 66 69 67 28 65 29 2c 74 68 69 73 2e 5f 73 65 6c 65 63 74 6f 72 3d 74 68 69 73 2e 5f Data Ascii: t-group-item",pn=".",dropdown",vn=".",dropdown-item",yn=".",dropdown-toggle",En="offset",Cn="position",T n=function(){function n(t,e){var n=this;this._element=t,this._scrollElement="BODY"===t.tagName?window:t,this._config=thi s._getConfig(e),this._selector=this._
2022-07-01 14:30:01 UTC	372	IN	Data Raw: 67 65 74 73 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 61 63 74 69 76 65 54 61 72 67 65 74 3d 6e 75 6c 6c 2c 74 68 69 73 2e 5f 73 63 72 6f 6c 6c 48 65 69 67 68 74 3d 6e 75 6c 6c 7d 2c 74 2e 5f 67 65 74 43 6f 6e 66 69 67 3d 66 75 6e 63 74 69 6f 6e 28 74 29 7b 69 66 28 22 73 74 72 69 6e 67 22 21 3d 74 79 70 65 6f 66 28 74 3d 6c 28 7b 7d 2c 73 6e 2c 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 74 26 26 74 3f 74 3a 7b 7d 29 29 2e 74 61 72 67 65 74 29 7b 76 61 72 20 65 3d 74 6e 28 74 2e 74 61 72 67 65 74 29 2e 61 74 74 72 28 22 69 64 22 29 3b 65 7c 7c 28 65 3d 46 6e 2e 67 65 74 55 49 44 28 65 6e 29 2c 74 6e 28 74 2e 74 61 72 67 65 74 29 2e 61 74 74 72 28 22 69 64 22 2c 65 29 29 2c 74 2e 74 61 72 67 65 74 3d 22 23 22 2b 65 7d 72 65 74 75 72 6e 20 46 6e 2e 74 79 Data Ascii: gets=null,this._activeTarget=null,this._scrollHeight=null),t._getConfig=function(t){if("string"!==typeof t&&(t={},sn,"obj ect"!==typeof t&&t?t:)).target){var e=tn(t.target).attr("id");e (e=Fn.getUID(en),tn(t.target).attr("id",e)),t.target="#"+e)return Fn.ty
2022-07-01 14:30:01 UTC	373	IN	Data Raw: 2c 22 29 3b 74 3d 74 2e 6d 61 70 28 66 75 6e 63 74 69 6f 6e 28 74 29 7b 72 65 74 75 72 6e 20 74 2b 27 5b 64 61 74 61 2d 74 61 72 67 65 74 3d 22 27 2b 65 2b 27 22 5d 2c 27 2b 2b 27 2b 65 2b 27 22 5d 27 7d 29 3b 76 61 72 20 6e 3d 74 6e 28 5b 5d 2e 73 6c 69 63 65 2e 63 61 6c 6c 28 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 74 2e 6a 6f 69 6e 28 22 2c 22 29 29 29 3b 6e 2e 68 61 73 43 6c 61 73 73 28 63 6e 29 3f 28 6e 2e 63 6c 6f 73 65 73 74 28 70 6e 29 2e 66 69 6e 64 28 79 6e 29 2e 61 64 64 43 6c 61 73 73 28 68 6e 29 2c 6e 2e 61 64 64 43 6c 61 73 73 28 68 6e 29 29 3a 28 6e 2e 61 64 64 43 6c 61 73 73 28 68 6e 29 2c 6e 2e 70 61 72 65 6e 74 73 28 64 6e 29 2e 70 72 65 76 28 67 6e 2b 22 2c 20 22 2b 6d Data Ascii: .);t=t.map(function(t){return t+[data-target="+e+"],'+'+[href="+e+""]});var n=tn(l.slice.call(document.querySe lectorAll(t.join(", ")));n.hasClass(cn)?(n.closest(pn).find(yn).addClass(hn),n.addClass(hn)):n.addClass(hn),n.parents(d n).prev(gn+", "+m
2022-07-01 14:30:01 UTC	375	IN	Data Raw: 3d 22 73 68 6f 77 22 2c 6a 6e 3d 22 2e 64 72 6f 70 64 6f 77 6e 22 2c 48 6e 3d 22 2e 6e 61 76 2c 20 2e 6c 69 73 74 2d 67 72 6f 75 70 22 2c 4c 6e 3d 22 2e 61 63 74 69 76 65 22 2c 52 6e 3d 22 3e 20 6c 69 20 3e 20 2e 61 63 74 69 76 65 22 2c 78 6e 3d 27 5b 64 61 74 61 2d 74 6f 67 67 6c 65 3d 22 74 61 62 22 5d 2c 20 5b 64 61 74 61 2d 74 6f 67 67 6c 65 3d 22 70 69 6c 6c 22 5d 2c 20 5b 64 61 74 61 2d 74 6f 67 67 6c 65 3d 22 69 73 74 22 5d 27 2c 57 6e 3d 22 2e 6 4 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 22 2c 55 6e 3d 22 3e 20 2e 64 72 6f 70 64 6f 77 6e 2d 6d 65 6e 75 20 2e 61 6 3 74 69 76 65 22 2c 71 6e 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 69 28 74 29 7b 74 68 69 73 2e 5f 65 6c 65 6d 65 6e 74 3d 74 7d 76 61 72 20 74 3d 69 2e 70 72 6f Data Ascii: ="show",jn=".",dropdown",Hn=".",nav, .list-group",Ln=".",active",Rn="> li > .active",xn="[data-toggle="tab"]", [data- toggle="pill"]", [data-toggle="list"], Wn=".",dropdown-toggle",Un="> .dropdown-menu .active",qn=function(){function i(t){ this._element=t}var t=i.pro

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	376	IN	Data Raw: 28 72 29 3b 62 6e 28 72 29 2e 6f 6e 65 28 46 6e 2e 54 52 41 4e 53 49 54 49 4f 4e 5f 45 4e 44 2c 73 29 2e 65 6d 75 6c 61 74 65 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 61 29 7d 65 6c 73 65 20 73 28 29 7d 2c 74 2e 5f 74 72 61 6e 73 69 74 69 6f 6e 43 6f 6d 70 6c 65 74 65 3d 66 75 6e 63 74 69 6f 6e 28 74 2c 65 2c 6e 29 7b 69 66 28 65 29 7b 62 6e 28 65 29 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 50 6e 2b 22 20 22 2b 4e 6e 29 3b 76 61 72 20 69 3d 62 6e 28 65 2e 70 61 72 65 6e 74 4e 6f 64 65 29 2e 66 69 6e 64 28 55 6e 29 5b 30 5d 3b 69 26 26 62 6e 28 69 29 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 4e 6e 29 2c 22 74 61 62 22 3d 3d 3d 65 2e 67 65 74 41 74 74 72 69 62 75 74 65 28 22 72 6f 6c 65 22 29 26 26 65 2e 73 65 74 41 74 74 72 69 62 75 74 65 28 22 61 72 69 61 2d Data Ascii: (r);bn(r).one(Fn.TRANSITION_END,s).emulateTransitionEnd(a))else s{}),t._transitionComplete=function(t,e,n){if(e){bn(e).removeClass(Pn+" "+Nn);var i=bn(e.parentNode).find(Un)[0];i&&bn(i).removeClass(Nn),"tab"===e.getAttribute("role")&&e.setAttribute("aria-
2022-07-01 14:30:01 UTC	377	IN	Data Raw: 6e 65 77 20 45 72 72 6f 72 28 22 42 6f 6f 74 73 74 72 61 70 27 73 20 4a 61 76 61 53 63 72 69 70 74 20 72 65 71 75 69 72 65 73 20 61 74 20 6c 65 61 73 74 20 6a 51 75 65 72 79 20 76 31 2e 39 2e 31 20 62 75 74 20 6c 65 73 73 20 74 68 61 6e 20 76 34 2e 30 2e 30 22 29 7d 28 65 29 2c 74 2e 55 74 69 6c 3d 46 6e 2c 74 2e 41 6c 65 72 74 3d 4b 6e 2c 74 2e 42 75 74 74 6f 6e 3d 4d 6e 2c 74 2e 43 61 72 6f 75 73 65 6c 3d 51 6e 2c 74 2e 43 6f 6c 6c 61 70 73 65 3d 42 6e 2c 74 2e 44 72 6f 70 64 6f 77 6e 3d 56 6e 2c 74 2e 4d 6f 64 61 6c 3d 59 6e 2c 74 2e 50 6f 70 6f 76 65 72 3d 4a 6e 2c 74 2e 53 63 72 6f 6c 6c 73 70 79 3d 5a 6e 2c 74 2e 54 61 62 3d 47 6e 2c 74 2e 54 6f 6f 6c 74 69 70 3d 7a 6e 2c 4f 62 6a 65 63 74 2e 64 65 66 69 6e 65 50 72 6f 70 65 72 74 79 28 74 2c 22 5f Data Ascii: new Error("Bootstrap's JavaScript requires at least jQuery v1.9.1 but less than v4.0.0")(e),t.Util=Fn,t.Ale rt=Kn,t.Button=Mn,t.Carousel=Qn,t.Collapse=Bn,t.Dropdown=Vn,t.Modal=Yn,t.Popover=Jn,t.Scrollspy=Zn,t.Tab=Gn,t.Tooltip=zn,Object.defineProperty(t,"_
2022-07-01 14:30:01 UTC	378	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49829	104.18.28.243	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	306	OUT	GET /icon/free/png-512/microsoft-sharepoint-3-599372.png HTTP/1.1 Host: cdn.iconscout.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://eyecandylashcompany.com/payment/frontend_paper_lantern/index.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-07-01 14:30:01 UTC	378	IN	HTTP/1.1 200 OK Date: Fri, 01 Jul 2022 14:30:01 GMT Content-Type: image/webp Content-Length: 4756 Connection: close Access-Control-Allow-Headers: DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Accept,X-CSRF-TOKEN,Authorization,Client-ID Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Allow-Origin: * Access-Control-Expose-Headers: Content-Length,Content-Range Cf-Bgq: imgq:100,h2pri Cf-Polished: origFmt=png, origSize=9488 Content-Disposition: inline; filename="microsoft-sharepoint-3-599372.webp" Vary: Accept etag: "7587997a8c364420c01dee48d83c6dcd" last-modified: Wed, 05 Feb 2020 05:33:45 GMT x-amz-meta-fl-original-last-modified: 2018-07-20T10:07:28Z CF-Cache-Status: HIT Age: 320852 Expires: Sat, 01 Jul 2023 14:30:01 GMT Cache-Control: public, max-age=31536000 Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Server: cloudflare CF-RAY: 723fd6531ef4bbd3-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
2022-07-01 14:30:01 UTC	379	IN	Data Raw: 52 49 46 46 8c 12 00 00 57 45 42 50 56 50 38 4c 80 12 00 00 2f ff c1 7f 10 f7 27 26 4d d6 3f bb 78 47 08 08 4a 24 29 7a 66 15 f6 b0 6d 7f a5 34 fa ce 0c 8c 48 07 65 45 53 60 b1 26 c4 b6 a8 b1 12 d7 90 86 2d 12 74 0d 91 54 6b 62 49 b1 ac 44 44 31 a2 69 f6 8a 2d 56 42 48 42 62 4c 96 b8 46 71 11 1b 62 42 82 a8 04 bb a2 52 06 91 36 cc cc f9 fe 39 b3 11 7e e7 77 7e e5 2f 22 fa 3f 01 d0 e2 ff 16 ff b7 f8 bf c5 ff 2d fe 6f f1 7f 8b ff 5b fc 2f 00 7d a3 16 17 22 81 92 4a e9 f6 da a6 02 27 92 29 a1 02 a2 12 0f 54 22 c1 72 c9 1c fe 56 6a a1 13 09 97 47 81 cf 26 65 59 51 8f 52 c8 1c 3e 31 b5 d0 89 7a 95 3e 81 cf 2e ca b2 a2 ae 65 8e b9 fb e4 ed 45 2a ea 5e d6 04 46 27 1f ac 46 3a 4a 18 73 f7 29 db 8b 54 a4 a7 64 09 8c 4e 3e 58 8d 94 95 27 e6 de 53 77 16 a9 48 61 39 Data Ascii: RIFFWEBPVP8L'/&M?xGJ\$)zfm4HeES`-&tTkbIDD1i-VBHBbLFqbBR69~w-l'?-o[/]"J")T*rVJG&eYQR>1z>.e E**F'F:Js)TdN>X'SwHa9

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	379	IN	Data Raw: 97 15 96 88 e9 3b 8b d1 18 65 44 fb d1 cb b3 6b d0 38 25 83 25 62 fa ee 12 34 58 89 d0 7e f4 f2 ec 1a 34 60 39 60 e9 3b 6b 77 09 1a b5 f8 eb 10 f3 49 4e 1d 1a b9 d0 b3 f4 9d 95 76 19 0d 5f d8 75 88 f9 34 a7 1e 99 50 c4 59 fa ce 4a bb 82 ec 28 da 1e 8e 5d 91 6b 43 b6 14 68 96 01 ef a5 df 40 06 15 64 0f c7 ae cc b5 21 a3 8a 2f cb 80 f7 d2 6f 20 cb 8a ad d0 71 ab 4e 35 22 eb 0a 2b 8f c1 b3 33 4a 91 89 85 54 e8 b8 55 a7 1a 91 99 45 93 c7 e0 d9 19 a5 c8 d6 02 49 09 8b 5b 93 d7 88 8c a9 16 6d 17 64 5e 91 f3 32 6f 23 6b 56 1c 48 7c 36 00 40 7c 29 61 71 6b f3 ec c8 98 f6 fc f5 f1 dd c0 b5 d8 f2 8a 9c 97 79 1b 59 f3 56 e6 9c 48 2f f8 ab c2 4a e9 14 bf 31 cf 8e 8c 69 cb 5d 31 2e 14 1e 58 48 79 0f 4b d8 5f 86 ac 79 39 6d c6 00 77 68 52 d1 a4 74 8a df 94 ef 44 c6 bc Data Ascii: ;eDk8%%b4X~4'9';kwlNv_u4PYJ(jkCh@d/l/o qN5"+3JTUEl[md^2o#kVh]6@l)aqkyYVH/J1j]1.XHyK_y9mwh RTD
2022-07-01 14:30:01 UTC	380	IN	Data Raw: 3f 08 2a 7d d7 1f 08 6c 3d 6a ab 95 52 00 10 36 2d a3 b4 29 d4 73 db e3 db 01 f1 33 c9 b0 fa f1 50 17 24 d6 be d4 1b 48 6d 3d fe 08 ad b4 21 a3 e6 6f fd a5 f0 76 ad c3 7e bf ec cf 9c 8c cf 27 45 06 80 3e f7 11 81 89 3c 34 83 98 9b 03 81 e8 de 5f 34 50 8b 9e 3e 17 89 a8 9c 35 3a dc 8d 77 be 22 e5 7c 08 90 1e bc a8 8c 71 20 c2 46 82 b6 e1 cc ba 97 83 79 a6 94 90 1b 8f 82 0e 3d a7 5d 66 1b 98 4f 8a 56 3d 9b d4 9d 57 82 91 4c 7b 7f d0 a7 fb 6b 97 98 c6 7c 9c 20 ed 6f ef 06 72 c9 33 84 24 83 6e 5b cd b2 32 0c 84 db c8 42 ac db d6 95 43 66 92 71 d3 4b 3f 00 1d 32 18 06 92 48 43 74 a4 75 e5 8e cf c8 98 03 86 68 48 ad 8a 89 43 b4 6f 0c e2 8c 0c 22 9c 1d b8 05 5e d0 01 a2 75 9a 89 2b 72 88 f8 03 b8 c5 fb 0b 5d 20 66 77 e2 89 73 44 7c c1 2d bd 2f a0 5e ab e3 39 a2 Data Ascii: ?*)=jR6-)s3P\$Hm=lov~'E'><4_4P>5:w"l[q Fy=]fOV=WL[k] or3\$[2BCfqk?2HctuhHCo"^u+r] fwsDl/-'9
2022-07-01 14:30:01 UTC	382	IN	Data Raw: 21 5e 1d ab a7 81 2a 19 e3 99 64 11 12 ef f8 b2 b2 b0 ab ce 10 0f f7 d4 8d e9 24 92 d9 83 45 c2 6d a4 d5 6e ea 02 2c ab 3b 74 ee eb a2 93 e9 48 66 ad 1b 83 98 8f 23 d9 05 b3 02 81 6d f5 87 68 df dd 5d 0f 83 6c 84 ea 02 83 24 20 c1 6a fe c2 70 60 5e 1a 20 aa 3f 3c a7 90 d6 bf 0a 09 5d ca 20 11 36 52 ea f3 d6 8c 6f 07 2c 4c 07 44 bc f0 41 07 a2 5e ad 45 52 87 b2 87 cf 45 24 b1 72 d6 a8 c7 dc 80 95 a9 81 d8 f8 dd 58 2f 52 ba fc 80 c4 56 59 e8 11 32 3a 61 db e1 73 77 ea 1c 8e ba ca 2b 27 bf 5f fd ce 33 41 3a d9 87 44 26 02 4b 53 04 11 6b d3 5f 69 4b 40 8f 9d 8d 48 ee 0e a0 43 d8 b4 8c 52 6c ca 92 3d 6f 3e 4c de 2c 24 d2 ea c7 6d 88 e8 c8 5d 12 e5 d5 1c 41 53 73 55 24 f9 79 1a 74 4d c8 c7 e6 2c 58 d0 99 ac a1 76 32 16 02 cf 69 1d 05 5b 67 3c f3 88 e9 c1 1e 19 Data Ascii: !^*d+\$Emn.,tHf#mh]j\$ jp^ ^?<j 6Ro,LDA^ERE\$R/RVY2:asw+ '_3A:D&KSk_iK@HCRI=o>L,\$m]ASsU\$ytM ,Xv2i[g<
2022-07-01 14:30:01 UTC	383	IN	Data Raw: b0 bf 8c 25 b4 6a c9 ee b7 23 dc 85 99 56 e9 14 bf 36 cf ce 10 2e eb 72 3e 8e 7d 48 98 b9 f4 8a 9c 97 79 9b 25 5c 5e 4f 7f 7f b0 87 30 d3 2a 61 71 6b f3 ec 2c a1 b5 e5 ad 8e 0b 13 66 2e bd 22 e7 65 de 66 09 97 77 f7 ff 3b ca 47 98 69 95 b0 b8 f5 67 ed 2c a1 75 14 6c 14 68 2e 3d 06 cf ce 28 65 09 22 45 93 cb d0 71 ab 4e 35 4a 3d ad c7 e0 d9 19 a5 52 cf 65 e8 b8 55 a7 1a a5 9e d6 32 e0 bd f4 1b 52 cf e5 c3 b1 2b 73 6d 52 4f 6b 19 f0 5e fa 0d a9 e7 f2 e1 d8 15 b9 36 a9 a7 b5 f4 9d 95 76 45 ea b9 ec 10 f3 69 4e bd d4 d3 5a fa ce 4a bb 2c f5 5c 76 88 f9 24 a7 4e ea 69 2d 11 d3 77 97 48 3d 97 ed 47 2f cf ae 91 7a 5a 4b c4 f4 dd 25 52 cf 65 fb d1 cb b3 6b a4 9e d6 12 31 7d 67 b1 d4 73 19 34 32 e5 50 8d d4 d3 ba f5 9e ba b3 58 ea b9 6c 3b 32 e5 50 8d d4 d3 9a 7b Data Ascii: %gj#V6.r>}Hy%\'^O0*aqk,f."efw;Gig,ulh.=(e"EgN5J=ReU2R+smROK^6vEiNZJ,\v\$Ni-wH=G/zZK%Rek1]js 42PXl;2P{

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49823	69.49.244.155	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-07-01 14:30:01 UTC	409	OUT	GET /payment/frontend_paper_lantern/images/office3651.png HTTP/1.1 Host: eyecandylashcompany.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://eyecandylashcompany.com/payment/frontend_paper_lantern/index.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-07-01 14:30:01 UTC	411	IN	HTTP/1.1 200 OK Date: Fri, 01 Jul 2022 14:30:00 GMT Server: Apache Last-Modified: Sat, 18 Jan 2020 17:50:20 GMT Accept-Ranges: bytes Content-Length: 18147 Connection: close Content-Type: image/png
2022-07-01 14:30:01 UTC	411	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 bb 00 00 00 bc 08 06 00 00 00 20 95 df d2 00 00 00 20 63 48 52 4d 00 00 7a 26 00 00 80 84 00 00 fa 00 00 00 80 e8 00 00 75 30 00 00 ea 60 00 00 3a 98 00 00 17 70 9c ba 51 3c 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 09 70 48 59 7 3 00 00 0b 13 00 00 0b 13 01 00 9a 9c 18 00 00 3a ee 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 0a 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d Data Ascii: PNGiHDR cHRMz&u0`pQ<sRGBgAMAapHYs:iTXtXML:com.adobe.xmp<?xpacket begin="" id="W5M0MpCe hiHzreSzNTczkc9d"?><x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk=

File Activities
Registry Activities

Analysis Process: splwow64.exe PID: 6548, Parent PID: 6356

General	
Target ID:	1
Start time:	16:28:44
Start date:	01/07/2022
Path:	C:\Windows\splwow64.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\splwow64.exe 12288
Imagebase:	0x7ff69a910000
File size:	130560 bytes
MD5 hash:	8D59B31FF375059E3C32B17BF31A76D5
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	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Completion	Count	Source Address	Symbol
------------------	---------------	---------------	-------------------	--------------	-----------------------	---------------

Analysis Process: chrome.exe PID: 1828, Parent PID: 1468

General	
Target ID:	19
Start time:	16:29:53
Start date:	01/07/2022
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 "https://eyecandylashcompany.com/payment/frontend_paper_lantern/index.html
Imagebase:	0x7ff7f6290000
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: 4908, Parent PID: 1828	
General	
Target ID:	20
Start time:	16:29:55
Start date:	01/07/2022
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=1572,25840 16860965793630,9285400582768245070,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1916 /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
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

Analysis Process: chrome.exe PID: 6864, Parent PID: 6356	
General	
Target ID:	26
Start time:	16:30:40
Start date:	01/07/2022
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 -- "https://eyecandylashcompany.com/payment/frontend_pap_er_lantern/index.html
Imagebase:	0x7ff7f6290000
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

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

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

Analysis Process: chrome.exe PID: 4944, Parent PID: 6864

General

Target ID:	27
Start time:	16:30:43
Start date:	01/07/2022
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=1492,14547 596045636120040,8967704105705094900,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1932 /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
Reputation:	high

Disassembly

 No disassembly