ID: 404286
Sample Name:
reflective_practice_template_nhs[1].pdf
Cookbook:
defaultwindowspdfcookbook.jbs
Time: 21:36:19
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

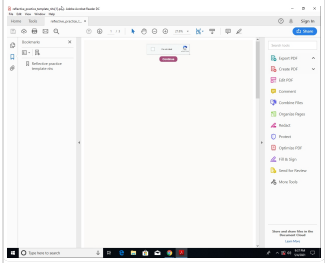
Analysis Report reflective_practice_template_nhs[1].pdf

Overview

General Information

Sample Name:	reflective_practice_template_nhs[1].pdf
Analysis ID:	404286
MD5:	bd93c6b39cf6fbf…
SHA1:	bc2b60452dbe49..
SHA256:	834c0a2229054d..
Infos:	

Most interesting Screenshot:



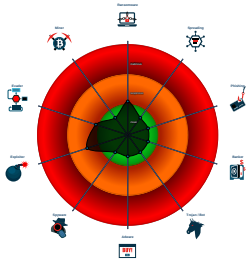
Detection

Score:	22
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- Machine Learning detection for samp…
- Contains functionality to access load…
- IP address seen in connection with o…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Analysis Advice

No malicious behavior found, analyze the document also on other version of Office / Acrobat

Uses HTTPS for network communication, use the 'Proxy HTTPS (port 443) to read its encrypted data' cookbook for further analysis

Startup

- **System is w10x64**
- AcroRd32.exe (PID: 6180 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\reflective_practice_template_nhs[1].pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 6268 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\reflective_practice_template_nhs[1].pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 6488 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6784 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1588,5207695692286208694,13668873235774985554,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=4477307787754487931 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=4477307787754487931 --renderer-client-id=2 --mojo-platform-channel-handle=1716 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6832 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1588,5207695692286208694,13668873235774985554,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --lang=en-US --gpu-preferences=KAAAAAAAAACAAwABAQAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=5528301929327232026 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6912 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1588,5207695692286208694,13668873235774985554,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=9756364306558423637 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=9756364306558423637 --renderer-client-id=4 --mojo-platform-channel-handle=1824 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 5984 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1588,5207695692286208694,13668873235774985554,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=7523555841818072242 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=7523555841818072242 --renderer-client-id=5 --mojo-platform-channel-handle=2224 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
  - chrome.exe (PID: 5228 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation -- 'https://traffking.ru/square?utm_term=reflective+practice+template+nhs' MD5: C139654B5C1438A95B321BB01AD63EF6)
    - chrome.exe (PID: 5564 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1560,17001144406219017590,14380291932932443674,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1824 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

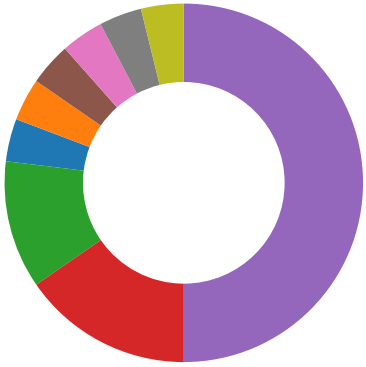
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion



Click to jump to signature section

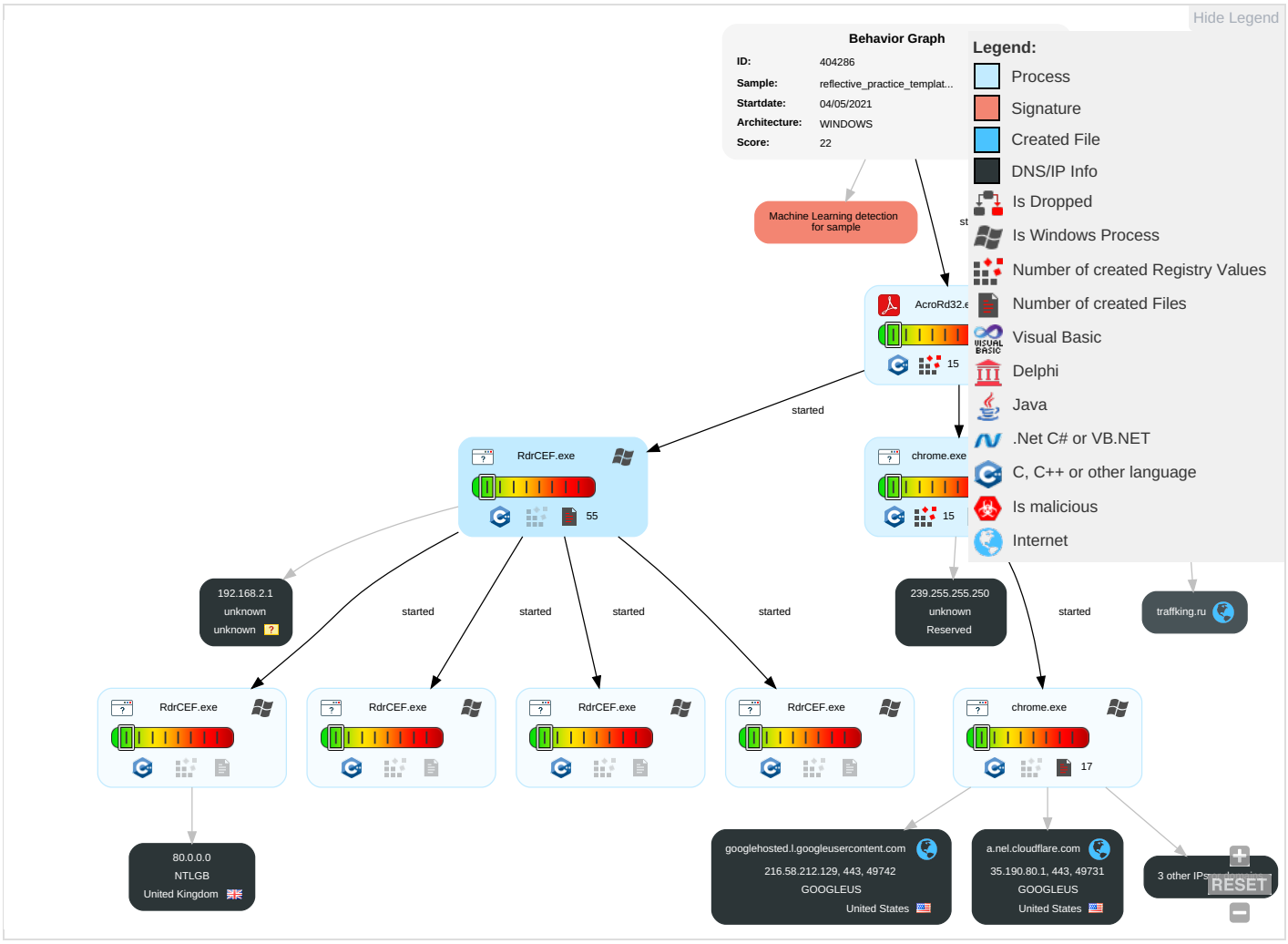
AV Detection:

Machine Learning detection for sample

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	Imp
Spearphishing Link 1	Exploitation for Client Execution 3	Path Interception	Process Injection 2	Masquerading 3	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sys Par
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Loc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da

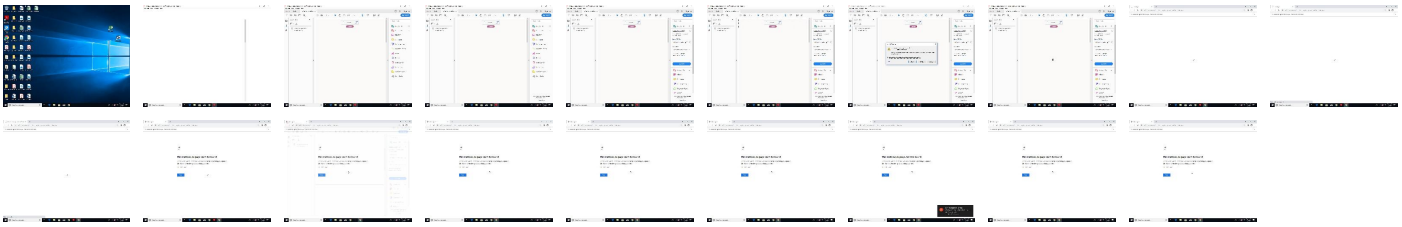
Behavior Graph

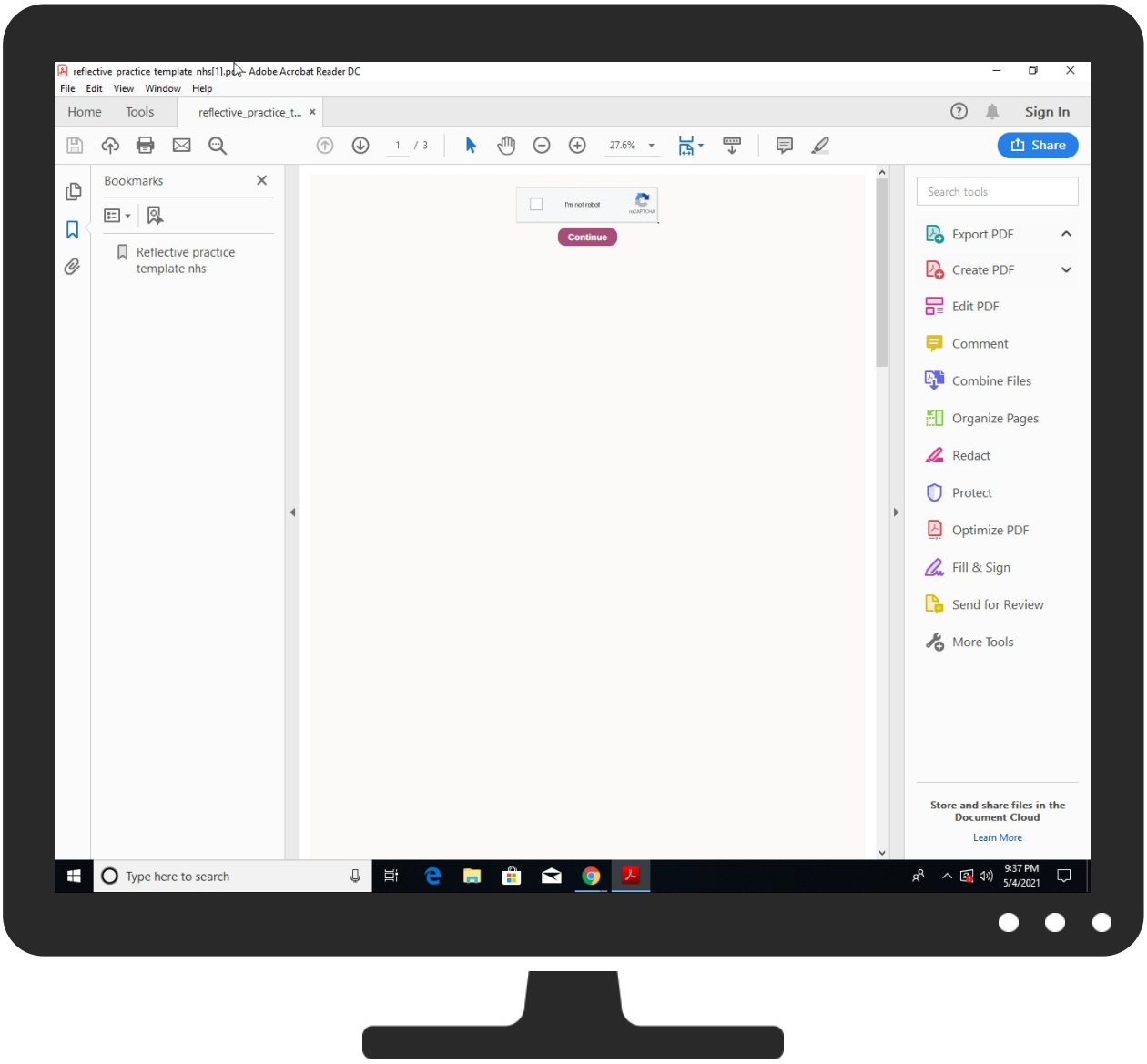


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
reflective_practice_template_nhs[1].pdf	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.sqhk.co/kilatelazobe/jetdOgd/retro_fridge_with_water_dispenser.pdf	0%	Avira URL Cloud	safe	
http://https://traffking.ru/square?utm_term=reflective	0%	Avira URL Cloud	safe	
http://https://api.echosign.com7	0%	Avira URL Cloud	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/ik	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/ma	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://cipa.jp/exif/1.0/	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/i	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/dfo	0%	Avira URL Cloud	safe	
http://https://cdn.sqhk.co/kapopajij/WiinigQ/protozoa_vs_bacteria_vs_virus_size.pdf	0%	Avira URL Cloud	safe	
http://https://cdn.sqhk.co/ludibipimilu/DhcRxOb/movie_software_for_windows_10.pdf)	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	0%	Avira URL Cloud	safe	
http://https://cdn.sqhk.co/ludibipimilu/DhcRxOb/movie_software_for_windows_10.pdf	0%	Avira URL Cloud	safe	
http://https://cdn.sqhk.co/kapopajij/WiinigQ/protozoa_vs_bacteria_vs_virus_size.pdf)	0%	Avira URL Cloud	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.osmf.org/drm/default	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/l	0%	Avira URL Cloud	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://https://api.echosign.comRL	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://https://cdn.sqhk.co/kilatelazobe/jetdOgd/retro_fridge_with_water_dispenser.pdf)	0%	Avira URL Cloud	safe	
http://https://cdn.sqhk.co/potexunajo/Qjajchj/hitman_2_silent_assassin_cheats.pdf)	0%	Avira URL Cloud	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://www.osmf.org/subclip/1.0	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/rlA	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/http://www.ascendercorp.com/http://www.ascendercorp.com/typedesigners.ht	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://www.fontbureau.comhttp://www.fontbureau.com/designersNegritaAgency	0%	Avira URL Cloud	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://ns.useplus.org/ldf/xmp/1.0/	0%	URL Reputation	safe	
http://www.ascendercorp.com/	0%	URL Reputation	safe	
http://www.ascendercorp.com/	0%	URL Reputation	safe	
http://www.ascendercorp.com/	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/$	0%	Avira URL Cloud	safe	
http://https://.OKCancelEdit	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://www.osmf.org/layout/anchor	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.npes.org/pdfx/ns/id/R	0%	Avira URL Cloud	safe	
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/Pk	0%	Avira URL Cloud	safe	
http://https://cdn.sqhk.co/kapopajij/WiinigQ/protozoa_vs_bacteria_vs_virus_size.pdfg-	0%	Avira URL Cloud	safe	
http://cipa.jp/exif/1.0/(15)8	0%	Avira URL Cloud	safe	
http://https://cdn.sqhk.co/potexunajo/Qjajchj/hitman_2_silent_assassin_cheats.pdf	0%	Avira URL Cloud	safe	
http://https://traffking.ru	0%	Avira URL Cloud	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	0%	URL Reputation	safe	
http://www.adobe.9	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/We9	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	0%	Avira URL Cloud	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://www.quicktime.com.Acrobat	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/4	0%	Avira URL Cloud	safe	
http://www.adobe.	0%	URL Reputation	safe	
http://www.adobe.	0%	URL Reputation	safe	
http://www.adobe.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
a.nel.cloudflare.com	35.190.80.1	true	false		high
traffking.ru	172.67.171.190	true	false		unknown
googlehosted.l.googleusercontent.com	216.58.212.129	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.sqhk.co/kilatelazobe/jetdOgd/retro_fridge_with_water_dispenser.pdf	AcroRd32.exe, 00000002.00000002.424349766.000000000B7AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://uploads.strikinglycdn.com/files/8c547329-0d1e-4dfa-b95f-2dc323cb86d4/world_war_one_weapons_c	AcroRd32.exe, 00000002.00000002.424135864.000000000B685000.00000004.00000001.sdmp, reflective_practice_template_nhs[1].pdf	false		high
http://www.aiim.org/pdfa/ns/field#Id	AcroRd32.exe, 00000002.00000002.427413592.000000000D56B000.00000004.00000001.sdmp	false		high
http://https://nalabusapigo.weebly.com/uploads/1/3/2/7/132740218/4175162.pdf)	reflective_practice_template_nhs[1].pdf	false		high
http://https://traffking.ru/square?utm_term=reflective	Current Session.21.dr	false	• Avira URL Cloud: safe	unknown
http://https://wosufixojiniki.weebly.com/uploads/1/3/4/7/134720754/4081785.pdf)	reflective_practice_template_nhs[1].pdf	false		high
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000002.00000002.427413592.000000000D56B000.00000004.00000001.sdmp	false		high
http://https://api.echosign.com7	AcroRd32.exe, 00000002.00000002.431160906.000000000E27C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/id/c	AcroRd32.exe, 00000002.00000002.431160906.000000000E27C000.00000004.00000001.sdmp	false		high
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000002.00000002.405944190.0000000007C70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://zopugazuf.weebly.com/uploads/1/3/4/6/134658021/6123242.pdf	AcroRd32.exe, 00000002.00000002.424349766.000000000B7AE000.00000004.00000001.sdmp	false		high
http://iptc.org/std/Iptc4xmpExt/2008-02-29/ik	AcroRd32.exe, 00000002.00000002.427413592.000000000D56B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

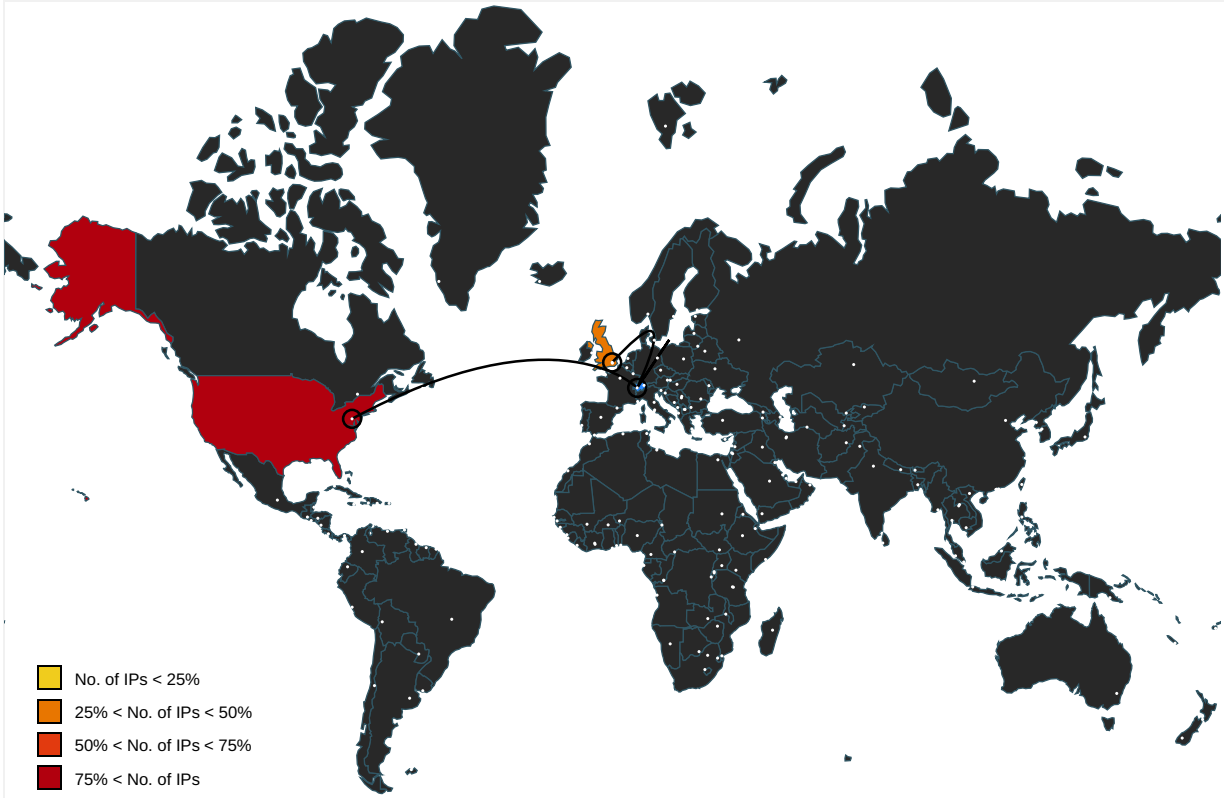
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://zoxiniguve.weebly.com/uploads/1/3/4/5/134584112/lunopamug_wemezuvulezurob.pdf	AcroRd32.exe, 00000002.00000002.423954231.000000000B595000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/ma	AcroRd32.exe, 00000002.00000002.423999541.000000000B5DB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://uploads.strikinglycdn.com/files/4371836f-f017-4f30-9831-11554ca34703/botunuxojok.pdf)	reflective_practice_template_nhs[1].pdf	false		high
http://https://gofolepoxi.weebly.com/uploads/1/3/4/8/134882907/7674727.pdf)	reflective_practice_template_nhs[1].pdf	false		high
http://https://zeginuvo.weebly.com/uploads/1/3/0/7/130775519/vapajukaba.pdf	AcroRd32.exe, 00000002.00000002.424349766.000000000B7AE000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000002.00000002.410868252.0000000009340000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/default/1.0%http://www.osmf.org/mediatype/default	AcroRd32.exe, 00000002.00000002.405944190.0000000007C70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://najijufo.weebly.com/uploads/1/3/4/7/134714833/pegloxufera_kudulavigiwub.pdf)	reflective_practice_template_nhs[1].pdf	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/i	AcroRd32.exe, 00000002.00000002.423999541.000000000B5DB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000002.00000002.427413592.000000000D56B000.00000004.00000001.sdmp	false		high
http://https://a.nel.cloudflare.com	4a93eb66-30ba-4de3-8ea0-312ddb38039b.tmp.22.dr	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/dfo	AcroRd32.exe, 00000002.00000002.431313305.000000000E686000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://zoxiniguve.weebly.com/uploads/1/3/4/5/134584112/lunopamug_wemezuvulezurob.pdf)	reflective_practice_template_nhs[1].pdf	false		high
http://https://tipefejiri.weebly.com/uploads/1/3/0/9/130969755/buwobu.pdf	AcroRd32.exe, 00000002.00000002.424349766.000000000B7AE000.00000004.00000001.sdmp	false		high
http://https://cdn.sqhk.co/kapopajij/WiinigQ/protozoa_vs_bacteria_vs_virus_size.pdf	AcroRd32.exe, 00000002.00000002.424349766.000000000B7AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.sqhk.co/ludibipimilu/DhcRxOb/movie_software_for_windows_10.pdf)	reflective_practice_template_nhs[1].pdf	false	• Avira URL Cloud: safe	unknown
http://https://api.echosign.com	AcroRd32.exe, 00000002.00000002.431160906.000000000E27C000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000002.00000002.423999541.000000000B5DB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://cdn.sqhk.co/ludibipimilu/DhcRxOb/movie_software_for_windows_10.pdf	AcroRd32.exe, 00000002.00000002.424349766.000000000B7AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.sqhk.co/kapopajij/WiinigQ/protozoa_vs_bacteria_vs_virus_size.pdf)	reflective_practice_template_nhs[1].pdf	false	• Avira URL Cloud: safe	unknown
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000002.00000002.431160906.000000000E27C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/drm/default	AcroRd32.exe, 00000002.00000002.405944190.0000000007C70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://zopugazuf.weebly.com/uploads/1/3/4/6/134658021/6123242.pdf)	reflective_practice_template_nhs[1].pdf	false		high
http://www.npes.org/pdfx/ns/id/l	AcroRd32.exe, 00000002.00000002.431160906.000000000E27C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.echosign.comRL	AcroRd32.exe, 00000002.00000002.431160906.000000000E27C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	AcroRd32.exe, 00000002.00000002.405944190.0000000007C70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	AcroRd32.exe, 00000002.00000002.423732062.000000000B4B1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.sqhk.co/kilatelazobe/jetdOgd/retro_fridge_with_water_dispenser.pdf)	reflective_practice_template_nhs[1].pdf	false	• Avira URL Cloud: safe	unknown
http://https://zeginuvo.weebly.com/uploads/1/3/0/7/130775519/vapajukaba.pdf)	reflective_practice_template_nhs[1].pdf	false		high
http://www.aiim.org/pdfa/ns/extension/	AcroRd32.exe, 00000002.00000002.427413592.000000000D56B000.00000004.00000001.sdmp	false		high
http://scripts.sil.org/OFLhttp://scripts.sil.org/OFL	AcroRd32.exe, 00000002.00000002.423732062.000000000B4B1000.00000004.00000001.sdmp	false		high
http://https://cdn.sqhk.co/potexunajo/Qjajchj/hitman_2_silent_assassin_cheats.pdf)	reflective_practice_template_nhs[1].pdf	false	• Avira URL Cloud: safe	unknown
http://https://gofolepoxi.weebly.com/uploads/1/3/4/8/134882907/7674727.pdf	AcroRd32.exe, 00000002.00000002.424349766.000000000B7AE000.00000004.00000001.sdmp	false		high
http://www.osmf.org/subclip/1.0	AcroRd32.exe, 00000002.00000002.405944190.0000000007C70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://genigudepa.weebly.com/uploads/1/3/1/0/131070712/kasodopizafazakoxuk.pdf)	reflective_practice_template_nhs[1].pdf	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/rlA	AcroRd32.exe, 00000002.00000002.423999541.000000000B5DB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://nalabusapigo.weebly.com/uploads/1/3/2/7/132740218/4175162.pdfp-	AcroRd32.exe, 00000002.00000002.424349766.000000000B7AE000.00000004.00000001.sdmp	false		high
http://www.aiim.org/pdfa/ns/property#	AcroRd32.exe, 00000002.00000002.427413592.000000000D56B000.00000004.00000001.sdmp	false		high
http://www.ascendercorp.com/http://www.ascendercorp.com/http://www.ascendercorp.com/typedesigners.ht	AcroRd32.exe, 00000002.00000002.423732062.000000000B4B1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dns.google	ed8954d8-3f2b-4e1b-b29d-f26f5a04eaca.tmp.22.dr, 4a93eb66-30ba-4de3-8ea0-312ddb38039b.tmp.22.dr, 10b9cad4-7dff-4d1c-b1c2-32538d1f314b.tmp.22.dr, 1704ca54-9349-4cf0-ac97-9bff9f5ae3ef.tmp.22.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comhttp://www.fontbureau.com/designersNegritaAgency	AcroRd32.exe, 00000002.00000002.423999541.000000000B5DB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000002.00000002.427413592.000000000D56B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ascendercorp.com/	AcroRd32.exe, 00000002.00000002.423732062.000000000B4B1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pumoguviponurin.weebly.com/uploads/1/3/4/7/134773216/miretigegurugi.pdf	AcroRd32.exe, 00000002.00000002.411079859.0000000009425000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/$	AcroRd32.exe, 00000002.00000002.431313305.000000000E686000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.aiim.org/pdfa/ns/id/	AcroRd32.exe, 00000002.00000002.431160906.000000000E27C000.00000004.00000001.sdmp	false		high
http://https://.OKCancelEdit	AcroRd32.exe, 00000002.00000002.431436814.000000000E777000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://tipefejiri.weebly.com/uploads/1/3/0/9/130969755/buwobu.pdf)	reflective_practice_template_nhs[1].pdf	false		high
http://iptc.org/std/Iptc4xmpExt/2008-02-29/	AcroRd32.exe, 00000002.00000002.427413592.000000000D56B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.osmf.org/layout/anchor	AcroRd32.exe, 00000002.00000002.405944190.0000000007C70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://uploads.strikinglycdn.com/files/4371836f-f017-4f30-9831-11554ca34703/botunuxojok.pdfN	AcroRd32.exe, 00000002.00000002.423954231.000000000B595000.00000004.00000001.sdmp	false		high
http://https://wixotavu.weebly.com/uploads/1/3/4/7/134764887/2953325.pdfb.	AcroRd32.exe, 00000002.00000002.424349766.000000000B7AE000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 00000002.00000002.427413592.000000000D56B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.aiim.org/pdfe/ns/id/	AcroRd32.exe, 00000002.00000002.431160906.000000000E27C000.00000004.00000001.sdmp	false		high
http://www.npes.org/pdfx/ns/id/R	AcroRd32.exe, 00000002.00000002.431160906.000000000E27C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://a.nel.cloudflare.com/report?s=XgDtas6rxmQXi1NtYYQGGtjvlm1lLbMIYjkQIprM4iwF0ZZj3tp0ISGyKdYPkd	Reporting and NEL.22.dr	false		high
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/Pk	AcroRd32.exe, 00000002.00000002.427413592.000000000D56B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.sqhk.co/kapopajij/WiinigQ/protozoa_vs_bacteria_vs_virus_size.pdfg-	AcroRd32.exe, 00000002.00000002.424349766.000000000B7AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://najijufo.weebly.com/uploads/1/3/4/7/134714833/pegulouxfera_kudulavigiwub.pdf	AcroRd32.exe, 00000002.00000002.423954231.000000000B595000.00000004.00000001.sdmp	false		high
http://https://genigudepa.weebly.com/uploads/1/3/1/0/131070712/kasodopizafazakoxuk.pdf	AcroRd32.exe, 00000002.00000002.424349766.000000000B7AE000.00000004.00000001.sdmp	false		high
http://cipa.jp/exif/1.0/(15)8	AcroRd32.exe, 00000002.00000002.410868252.0000000009340000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.sqhk.co/potexunajo/Qjajchj/hitman_2_silent_assassin_cheats.pdf	AcroRd32.exe, 00000002.00000002.424349766.000000000B7AE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://traffking.ru	AcroRd32.exe, 00000002.00000002.431313305.000000000E686000.00000004.00000001.sdmp, 4a93eb66-30ba-4de3-8ea0-312ddb38039b.tmp.22.dr	false	• Avira URL Cloud: safe	unknown
http://https://wixotavu.weebly.com/uploads/1/3/4/7/134764887/2953325.pdf)	reflective_practice_template_nhs[1].pdf	false		high
http://www.aiim.org/pdfa/ns/field#	AcroRd32.exe, 00000002.00000002.427413592.000000000D56B000.00000004.00000001.sdmp	false		high
http://www.osmf.org/layout/padding%http://www.osmf.org/layout/attributes	AcroRd32.exe, 00000002.00000002.405944190.0000000007C70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nalabusapigo.weebly.com/uploads/1/3/2/7/132740218/4175162.pdf	AcroRd32.exe, 00000002.00000002.424349766.000000000B7AE000.00000004.00000001.sdmp	false		high
http://www.adobe.9	AcroRd32.exe, 00000002.00000002.431160906.000000000E27C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/We9	AcroRd32.exe, 00000002.00000002.423999541.000000000B5DB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://wixotavu.weebly.com/uploads/1/3/4/7/134764887/2953325.pdf	AcroRd32.exe, 00000002.00000002.424349766.000000000B7AE000.00000004.00000001.sdmp	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/	AcroRd32.exe, 00000002.00000002.431313305.000000000E686000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://clients2.googleusercontent.com	4a93eb66-30ba-4de3-8ea0-312ddb38039b.tmp.22.dr, 1704ca54-9349-4cf0-ac97-9bff9f5ae3ef.tmp.22.dr	false		high
http://www.quicktime.com.Acrobat	AcroRd32.exe, 00000002.00000002.405944190.0000000007C70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/4	AcroRd32.exe, 00000002.00000002.423999541.000000000B5DB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000002.00000002.410868252.0000000009340000.00000004.00000001.sdmp	false		high
http://https://wosufixojiniki.weebly.com/uploads/1/3/4/7/134720754/4081785.pdf	AcroRd32.exe, 00000002.00000002.424349766.000000000B7AE000.00000004.00000001.sdmp	false		high
http://scripts.sil.org/OFL	AcroRd32.exe, 00000002.00000002.423732062.000000000B4B1000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aiim.org/pdfa/ns/id/-	AcroRd32.exe, 00000002.00000002.431160906.000000000E27C000.00000004.00000001.sdmp	false		high
http://www.adobe.	AcroRd32.exe, 00000002.00000002.431313305.000000000E686000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.21.dr	false		high
http://https://uploads.strikinglycdn.com/files/4371836f-f017-4f30-9831-11554ca34703/botunuxojok.pdf	AcroRd32.exe, 00000002.00000002.423954231.000000000B595000.00000004.00000001.sdmp	false		high
http://https://pumoguviponurin.weebly.com/uploads/1/3/4/7/134773216/miretigegurugi.pdf)	reflective_practice_template_nhs[1].pdf	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.212.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.67.171.190	traffking.ru	United States		13335	CLOUDFLARENETUS	false
35.190.80.1	a.nel.cloudflare.com	United States		15169	GOOGLEUS	false
80.0.0.0	unknown	United Kingdom		5089	NTLGB	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond

Analysis ID:	404286
Start date:	04.05.2021
Start time:	21:36:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	reflective_practice_template_nhs[1].pdf
Cookbook file name:	defaultwindowspdfcookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	SUS
Classification:	sus22.winPDF@50/263@4/7
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .pdf • Found PDF document • Find and activate links • Security Warning found • Close Viewer

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 13.88.21.125, 40.88.32.150, 20.50.102.62, 131.253.33.200, 13.107.22.200, 93.184.220.29, 52.255.188.83, 23.57.80.111, 2.20.142.228, 2.20.143.130, 2.20.143.5, 2.20.142.203, 2.20.142.225, 2.20.142.226, 23.54.113.182, 204.79.197.200, 13.107.21.200, 23.54.113.53, 92.122.213.247, 92.122.213.194, 2.20.142.209, 2.20.142.210, 142.250.185.205, 142.250.185.78, 142.250.184.195, 142.250.185.206, 95.168.222.146, 34.104.35.123, 95.168.222.141, 142.250.186.74, 142.250.186.106, 142.250.186.138, 142.250.186.170, 142.250.184.202, 142.250.184.234, 172.217.18.106, 172.217.23.106, 216.58.212.138, 142.250.185.74, 172.217.16.138, 142.250.185.106, 142.250.185.138, 142.250.185.170, 142.250.185.202, 142.250.185.234, 20.54.26.129, 72.246.101.132, 172.217.23.99, 142.250.185.67, 52.155.217.156 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, cs9.wac.phicdn.net, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, acroipm2.adobe.com, skypedataprdcoleus15.cloudapp.net, clients2.google.com, ocsp.digicert.com, wildcard.weather.microsoft.com.edgekey.net, a122.dscd.akamai.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, update.googleapis.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, acroipm2.adobe.com.edgesuite.net, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, www.googleapis.com, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, edgedl.me.gvt1.com, store-images.s-microsoft.com, r2.sn-n02xgoxufvg3-2gbs.gvt1.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com, au.download.windowsupdate.com.edgesuite.net, e4578.dscb.akamaiedge.net, r2---sn-n02xgoxufvg3-2gbs.gvt1.com, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, e15275.g.akamaiedge.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, redirector.gvt1.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, accounts.google.com, tile-service.weather.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus17.cloudapp.net, r7.sn-n02xgoxufvg3-2gbs.gvt1.com, a-0001.a-afdentry.net.trafficmanager.net, armmf.adobe.com, r7---sn-n02xgoxufvg3-2gbs.gvt1.com, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile 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
21:37:24	API Interceptor	9x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
239.255.255.250	test.html	Get hash	malicious	Browse	
	PaymentAdvice - Copy.htm	Get hash	malicious	Browse	
	INVOICE & STATEMENTS -COPY.htm	Get hash	malicious	Browse	
	DGNTL04052021.2-8864.html	Get hash	malicious	Browse	
	referenceMemMem.hta	Get hash	malicious	Browse	
	Notes Received gcgaming.com.html	Get hash	malicious	Browse	
	Tree Top.html	Get hash	malicious	Browse	
	ATT51630.htm	Get hash	malicious	Browse	
	message for dtriscritti@discountwaste.com.html	Get hash	malicious	Browse	
	efax637637637.htm	Get hash	malicious	Browse	
	afafd.htm	Get hash	malicious	Browse	
	efax663663663.htm	Get hash	malicious	Browse	
	FedEx Shipment Address Update Form2021.html	Get hash	malicious	Browse	
	jdCsAaeOMw3AekTOgSZ92vgpOBC5TwWgMkt.html	Get hash	malicious	Browse	
	Cws-Pay Application.html	Get hash	malicious	Browse	
	.htm	Get hash	malicious	Browse	
	sean.adair@redwirespace.com1__redwirespace.com.htm	Get hash	malicious	Browse	
	FAXQKJEZPA42S.htm	Get hash	malicious	Browse	
	efax702702702.htm	Get hash	malicious	Browse	
	#Ud83d#Udcde.htm	Get hash	malicious	Browse	
80.0.0.0	Autofactura generada mes de Abril 27-04-2021.pdf.exe	Get hash	malicious	Browse	
	Autofactura generada mes de Abril 27-04-2021.pdf.exe	Get hash	malicious	Browse	
	1RIA_IT_Formazione di Base Compliance_IT.pdf.exe	Get hash	malicious	Browse	
	1RIA_IT_Formazione di Base Compliance_IT.pdf.exe	Get hash	malicious	Browse	
	123.exe	Get hash	malicious	Browse	
	123.exe	Get hash	malicious	Browse	
	EiK2ZuecHv.exe	Get hash	malicious	Browse	
	File6512365134_7863_20210413.html	Get hash	malicious	Browse	
	DHL_Express_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	
	DHL_Express_Shipment_Invoice_Confirmation_CBJ19051 7000131_74700456XXXX.exe	Get hash	malicious	Browse	
	DHL_Express_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	
	DHL_Express_Shipment_Confirmation_BKKR005545473_88 700456XXXX.exe	Get hash	malicious	Browse	
	APRILQUOTATION#QQO2103060_SAMPLES_KHANG HY_CO_CORPORATION.exe	Get hash	malicious	Browse	
	#U260f8284.HTML	Get hash	malicious	Browse	
	HunpuKMHQt.exe	Get hash	malicious	Browse	
	JbQoNNPVOk.exe	Get hash	malicious	Browse	
	_vm583573758.htm	Get hash	malicious	Browse	
	March 17, 2021, 101142 AM.HTM	Get hash	malicious	Browse	
	message_zdm.html	Get hash	malicious	Browse	
	0000001_Carved.pdf	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	j5lw25ifjr.dll	Get hash	malicious	Browse	• 104.20.185.68
	lxJ7l5vVmLx6QS7.exe	Get hash	malicious	Browse	• 172.67.188.154
	oUvjpbnwz3.dll	Get hash	malicious	Browse	• 104.20.185.68
	KdLJVb0Aoi.dll	Get hash	malicious	Browse	• 104.20.184.68
	PaymentAdvice - Copy.htm	Get hash	malicious	Browse	• 104.16.19.94
	INVOICE & STATEMENTS -COPY.htm	Get hash	malicious	Browse	• 104.16.126.175
	DGNTL04052021.2-8864.html	Get hash	malicious	Browse	• 104.16.19.94
	01_extracted.exe	Get hash	malicious	Browse	• 172.67.188.154
	iuCN1LJ980.dll	Get hash	malicious	Browse	• 104.20.185.68
	i6ALtgS6nV.dll	Get hash	malicious	Browse	• 104.20.184.68
	iwEcXUAues.dll	Get hash	malicious	Browse	• 104.20.184.68
	MOe7vYpWXW.exe	Get hash	malicious	Browse	• 23.227.38.74
	i6ALtgS6nV.dll	Get hash	malicious	Browse	• 104.20.184.68
	Proforma adjunta N#U00ba 42037,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	swift copy.exe	Get hash	malicious	Browse	• 104.21.19.200
	XmLE5f5wBX.dll	Get hash	malicious	Browse	• 104.20.185.68
	Presupuesto urgente PST56654256778982, pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Notes Received gcgaming.com.html	Get hash	malicious	Browse	• 104.16.18.94
	DHL 4677348255142.exe	Get hash	malicious	Browse	• 104.21.19.200
	BCJOphish040520219700.html	Get hash	malicious	Browse	• 104.16.18.94
NTLGB	8UsA.sh	Get hash	malicious	Browse	• 82.32.79.178
	x86_unpacked	Get hash	malicious	Browse	• 82.17.192.153
	Autofactura generada mes de Abril 27-04-2021.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	Autofactura generada mes de Abril 27-04-2021.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	rIbyGX66Op	Get hash	malicious	Browse	• 86.18.93.173
	1RIA_IT_Formazione di Base Compliance_IT.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	1RIA_IT_Formazione di Base Compliance_IT.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	J76uxxiy.exe	Get hash	malicious	Browse	• 86.18.99.199
	123.exe	Get hash	malicious	Browse	• 80.0.0.0
	123.exe	Get hash	malicious	Browse	• 80.0.0.0
	EiK2ZuecHv.exe	Get hash	malicious	Browse	• 80.0.0.0
	File6512365134_7863_20210413.html	Get hash	malicious	Browse	• 80.0.0.0
	DHL_Express_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	• 80.0.0.0
	DHL_Express_Shipment_Invoice_Confirmation_CBJ19051 7000131_74700456XXXX.exe	Get hash	malicious	Browse	• 80.0.0.0
	DHL_Express_Shipments_Invoice_Confirmation_CBJ1905 17000131_74700456XXX.exe	Get hash	malicious	Browse	• 80.0.0.0
	DHL_Express_Shipment_Confirmation_BKKR005545473_88 700456XXXX.exe	Get hash	malicious	Browse	• 80.0.0.0
	APRILQUOTATION#QQO2103060_SAMPLES_KHANG HY_CO_CORPORATION.exe	Get hash	malicious	Browse	• 80.0.0.0
	#U260f8284.HTML	Get hash	malicious	Browse	• 80.0.0.0
	HunpuKMHQt.exe	Get hash	malicious	Browse	• 80.0.0.0
	1.sh	Get hash	malicious	Browse	• 62.254.90.3

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

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	moderate, 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 GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	410
Entropy (8bit):	5.631963286078434
Encrypted:	false
SSDEEP:	6:men9YOFLvEWdM9QJ/l/Bv/i7Z+P41TK6tEen9YOFLvEWdM9QlAu/Ni7Z+P41TK6V:vDRM90/SZiEnDRM9AA7ZiEV
MD5:	4BB57DBA51FC77C82FCAA963296A2396
SHA1:	6CA39C2DEF431B1E5167E1E43895DE23A0F6FF85
SHA-256:	071952EBA7A768CE4F2E9FAFCB4C5C0DED17C7FAE8C2C7ADAADE4E354403F079
SHA-512:	65C08488333F149176F2DC7188E05C0BF8CA2086357D9112D6DEC4021041B56BFD3FBB49B44705EECE9D1A99CECBA99E6499FAE887EF3DBA2A61BC45187547
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M.....,_keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .....$ /....."#.D\v.D.$.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....cf.....0\r..m.....M.....,_keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ..N..$ /....."#.D.b.F.$.A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo.....G.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.569137326160573
Encrypted:	false
SSDEEP:	6:mi9NqEYOFLvEkot/oEi8Be7Ywcr1TK6tyoMi9NqEYOFLvEkFl//az8Be7Ywcr1TD:V9zGi9PQsoH9ziz9PQ
MD5:	F19CF255CA7BE8C9130BDC56F5CC2927
SHA1:	688798E6DA66F142D8CA23E9AB12B8C0B76F5794
SHA-256:	2C26F2BBA8F8327530631C020F185D7E6F5D55A201477481CCFCF5CAD72A13A1
SHA-512:	0814F5933CF0D37D6EE0CFE9DD51222FCA91A9BEE3E853442181ED0535C616A05425435926997707C55CE7E0FD62287FDF76DFEE044DB6AD99D7B90C5AAEC5F
Malicious:	false
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..k..$ /....."#.D...D.$.A.1.x.'.vI..*\|Z..o...+.4....0..A..Eo.....A..Eo.....Q.5.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..y..$ /....."#.DJ..E.$.A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....I .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	492
Entropy (8bit):	5.593123535626784
Encrypted:	false
SSDEEP:	12:DyeRVFAFjVFAFjE9vlUo6j7m5yeRVFAFjVFAFgPvlUo6j6:tB4v4wZSBq3B4v4gnSB
MD5:	47ECEC79E697ED8592C2508CC61D4824
SHA1:	33C11FFBE911E8D56C68D33E2914C9F03CB1BEE6

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
SHA-256:	1B3801DB5672CD182D312916649F9129E8F4CCB097B6E29342C1E63223322EF5
SHA-512:	D3A0ABA35B0B0A9F32ECBA3FDD03FF629F0368B0AECCE9D0F869F126C0FBD3F9E97C503288E6C9018BD90C684A2118A305634F9D9E129927E231AD5AFF9BA1B
Malicious:	false
Preview:	0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ....$ /....."#.D<g}D.$.A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .1x..$ /...."#.D...E.$.A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.619762637427953
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5RsZmt/RHiWulHyA1TK6t0:IbRkiDtCWussa
MD5:	4817DAC702193AD4180A1DBC4270846A
SHA1:	5E8546137B2D7751DC60303FE990887541605BDD
SHA-256:	B2251E73512616C10E7C495A8E7DDEE23F785AA02ED72BE7F224F5D72278AA9E
SHA-512:	AC5DB61899D06107CD4BF771BC8B51A239E8CBF4A01ABF1ED976EAB4F273127B4F5FD8A70404CA22747C6F7E0D9CBD21CD227DB770BA573027FC7EB7491D906
Malicious:	false
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .y7..$ /....."#.Dv..D.$.A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo.....A..Eo.....BUw.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.549774243016546
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVu1y/6PZDRVyh9PT41TK6tBY:pyixRupPZDRV41TEX
MD5:	9A80FF643736EE36A15163179676DCD7
SHA1:	03B0359DBB07BE9377A0C0E746C87C4B48749CB6
SHA-256:	28285DFB4569A5F44DFA17C18443082D448D6C4CD9A64347DD9D9A1EBDF0957A
SHA-512:	035673B83C414E16EFD6F7DBB8507C8BAA6FB5C3853BA6C7F80A43AC8453FD9E3A545D58960E95D72D4CE082F78503C320200F16611D0F040780B17FA143906D
Malicious:	false
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js .....$ /....."#.D...E.$.Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo. .....@.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.621647904682762
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQXtK/l/5qhLZll6P41TK6t:0RhkB/6hLZC
MD5:	67B892F78CF1F66E271DB89C206610D3
SHA1:	2214C8428C11133A8D5B4E1BE1355662E77AAECC
SHA-256:	451D876F4843313A942EA48654887162F6E85314A19EDAC0190A79CEEEEB06DB
SHA-512:	058E6953611A31A7179BC12B9268AB61F4AF5428626D81B25DB7400823D472F3D9F38349D68504D04D49F0D18EFE8B770AC117B9DCACA6ED7B561359C2E35345
Malicious:	false
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .^1..$ /....."#.D..E.$.A.].>....uUf..N...k.....c..l.A..Eo.....A. .Eo.....ML.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.506299101035559
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0	
SSDEEP:	6:mJYOFLvEWdGQRQOdQUsS//usXV6g1TK6tRAOll/:2RHRQCtsza1kO//
MD5:	5DA94A7AE9B2F5F802EC2BB89BD63305
SHA1:	C8E93945B49BC249649FBD59149776B8EDFC6A23
SHA-256:	00A2715B5084D2736D88D46EA8B64022E94C01183721C07A2D7426042252E902
SHA-512:	8F11BAA5A78CF58C30A5C2040A4D9000C613AFCD6F748FE9298348DA8071DD2B49C094942AAB399AA687F947D07070509B6324503A39292DD8D2E29A3131B61C
Malicious:	false
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ..H..$ /....."#.D(..E.$.A..c..y/L....|y.n..C/I.....X7-ne.A..Eo.....A..Eo .....rd%w.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.592293814937624
Encrypted:	false
SSDEEP:	6:mOYOFLvECMLP//hEhMuR/41TK6tH8OYOFLvECML+/nMuR/41TK6t3cFl:Z5M9+MuR/EJ75MGMuR/EVcF
MD5:	3EB283963E429975B848489E69693261
SHA1:	D5EE59E144C5077E3B22F2A45EF1508C6BCBCD77
SHA-256:	440FC29431DE7ABC3A114EC16095E68B325B177A97726DE4CADD31628BC22B2A
SHA-512:	5C7315473F48E7518F23A9060865B9B03815655F7D8F3FF078CFF9B8E31C6CD9BB9393EE3837D63B96D03155526D0A082FBA8455710745FE85367D0EFC327208
Malicious:	false
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..q..$ /....."#.D.,.D.$.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....A.....0\r..m.....3.... <lb...._keyhttps://rna-resource.acrobat.com/base_uris.js .....$ /....."#.D..E.$.A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....79.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.513749459842036
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtumKl//KBG01+by0zBUKSAA1TK6t3:pRxKlz01+beR
MD5:	9F51E3F1516A9FB719485B1E77A4B502
SHA1:	4FBAF633609F9035A2483C499237088289D27C23
SHA-256:	4F820BFC61D21BF1D519EFB3D5DC12A6B91D10746B49352D5D933C2CBF0E1725
SHA-512:	4BCDCF42DAC3639F57F7A5E0B2FC79CD16244B00928F6827983180EA8707CC3F2D085C9BCB1084FDD46D249A30BC6A34476F81BB46A0641383378D5D544BD05
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js .....$ /....."#.D.B.E.$.AQ..E.=....=h`t..t..3%A.F$..w..A..Eo..... .....A..Eo.....8.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	354
Entropy (8bit):	5.493064683834928
Encrypted:	false
SSDEEP:	6:md4HXXYOFLvEjMSWFvngQ/26p3tUdyP41TK6ted4HXXYOFLvEjMSWFvt/CtUdyPh:KkXxKMSCvng74tUlYkXxKMSCvktUl6
MD5:	ED913CC4DE8575D3D5E74715F9AC6761
SHA1:	390D6A8EAC87636CBB05721BCD122972E8756E78
SHA-256:	251E81D53C6EE9275C0A87B1379C32DA5386E547C9A12B66819F3ADC722BA2AD
SHA-512:	BBFD01C54B4F127D3D9677AA3BC1CC035EF2260DE56F461AFA8BBAB9F1A95A03EF991D2D25B5F04B0133FC9F7FCC2FB5031ADBA5FADC0A7315CB3E0B4E09E 3C4
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..n..$ /....."#.D...D.$.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....u.q.....0\r..m.....1 .....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..}..$ /....."#.D{.E.$.A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....Aa#.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	374

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0	
Entropy (8bit):	5.54525309073133
Encrypted:	false
SSDEEP:	6:mkl9YOFLvEWsfOL+mKt/JzumyyM+VY1TK6tbkl9YOFLvEWsfOL6li/o1yyM+VY13:5h6OL8nzdkWh6OL2Xk
MD5:	E9BA46DD99D930BC74ED0B69DD7AF121
SHA1:	5E6CA5620D1DC9E9AA34E8FDCD5BE37F64406387
SHA-256:	7C12DE1845459C1583C23D3A13AB18BFCD82157F6513B2518173F49C3015A18E
SHA-512:	861BF586DF3724C99D438AB994B448FF8D2542C19BDDB3A81C8A3D3589F7F9B974EEA6FF9F98D7670B57925BF701E4CC6E333E987214C9390150D504A986F65C
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ."...$ /....."#.D0.[D.$.A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....8.....0\r..m.....;..I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .....$ /....."#.D.G.E.$.A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....z.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	488
Entropy (8bit):	5.584891989953156
Encrypted:	false
SSDEEP:	12:URVFAFjVFAFeJVwSeKaTLnQLRVFAFjVFAFzK+wSeKaTLn:UB4v4UwzXLneB4v4rwzXLn
MD5:	043AAB6FCCC558E1E5C08CD95293B632
SHA1:	406ABE6507C37CAE04FF9CBF9710AD703FE2F0F8
SHA-256:	F40323CF813B38B709E4576BEDDD5C5AF9A38750591FA2FC42901980221E08EC
SHA-512:	D9D822985158CA6F09F8D06BEA78064860C10D632325F6E8AEBE5F5D1555F55BCD61920A6E517C60B27D1E2E4C83772D9A37809DC205B771567A247A9B820731
Malicious:	false
Preview:	0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js .i...$ /....."#.D..D.$.A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js .h...$ /....."#.De..F.$.A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....D.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.469776000687835
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXuxJsi/xMtP11TK6tB:BsR2EseteMPP
MD5:	8048E3DA03DF92773353EE83CFDA4A39
SHA1:	9415540E85C31D974FA7B2E0765CB0754521DF5D
SHA-256:	2BBD46E8010078A8EA81BFA4DFCC9F8C9ABAB3C94DDCE16913BA925699D4733D
SHA-512:	2ED91133181500E1FC032BA829C409D8847EDB34BE773AF7AEA24AAE0D0161F893EB7E2C21138D8615E2477D68BE6108F34E9703C1E89638D5AE1133482CEFA(
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .>...$ /....."#.Dg..E.$.A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.....w@.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.627644132360778
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQBsWl/Z3B7OhKlvA1TK6t:RbR16FW33BJk
MD5:	D0E0413C60FB54DC9C25EBE8E160D84C
SHA1:	B85498B6B6171DFD53286834E72D25B60D4B40D0
SHA-256:	B9AA722E708EBE76E30EC48992289A5C93FADFA162113009E4BCDEF650BBC109
SHA-512:	65E3C0D82E32129FCE9359ACECDE22AE650A8002FC7255DBAEC8F8316133ECE1DD026B7B6920A5E5DDF2FBD34632B701D57F99C6570741622EE73A1E8635DA6
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ..)..$ /....."#.D.;.E.$.A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....;.s.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.558552303606602
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVu/mt/ZG6nQdFt1TK6tNH:B2geRHRQlmHGu0b
MD5:	EE4C70D1538F5090ED8D678D06DFCE9C
SHA1:	7169411C29F7A50071264E2E9A7935A1455B4247
SHA-256:	51564E00EB97E6146A250DCAEB9DC1989AB97A03A99F6CD9E5A3963948E93C9A
SHA-512:	A246D9272C72A827608918C711685DC97FB5839B941E8C623C745FD6759E2818C340140441F2E1A7CD81E7D3930F22DD6FE33404899A9C11DEFBFB49321AB70C
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .l...$ /....."#.D+..E.$.A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A. .Eo.....U74N.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	412
Entropy (8bit):	5.619768148973
Encrypted:	false
SSDEEP:	6:mzyEYOFLvEWdrIOQLKt/ev56t1S/1TK6tyEzyEYOFLvEWdrIOQsl//Ul9r56t1SF:WyeRlq6t1wkMyeRl0156t1wrH
MD5:	41346F9E107CEF1968F1BF3C534BCE43
SHA1:	EC97A08CD608EF8E36A06A0F7B1BA07565C7B66A
SHA-256:	91C953FC2C80245CA97F86012AF2170E14F593D4BE72AD96DB08F81CDE6CAAF8
SHA-512:	8AA744FC6CF732E2946B738E48432C697366D1C7A800A2A27D3551895891561C72A71ECDA13B8DFF6EA41F53082DDD60F23DEB5B2FEF90D1CFF15972CC59102
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..q..$ /....."#.Dc.hD.$.A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.... ..F;.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..9..$ /....."#.D.T.E.$.A.t\a.....x5.'OuE.C..@.....x..A..Eo..... .....A..Eo.....+.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.490664004001275
Encrypted:	false
SSDEEP:	3:m+lKcv8RzYOCGLvHkWBGKuKjXKoyNH/KPWFvdWlll0NYNqww6U+5m1TK5ktf1:mnYOFLvEWdhwyuyl/usqwK+41TK6t
MD5:	CFBEABFADE6C70FFC9646E42834AA03E
SHA1:	14B4FABA2F9CE83EAE3C0017026489A71C0565CC
SHA-256:	8CAD39321F795AD8C31CCF015F4D646682095F0A1B9D186BBCBFADEF161E0B89
SHA-512:	E4A47720BE2A928FFD68C924B7C529299510DB276E5F48A43796F083AB844FAF46BF68E9DC74F8CBDD16B48094893A9815C46688ECCC39519D13F934E10C9E9
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .m...$ /....."#.DG..E.$.A.....7...o..a=.98I.....(3.$G.A..Eo..... ...A..Eo.....w.q6.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	460
Entropy (8bit):	5.61523139184034
Encrypted:	false
SSDEEP:	6:mYXYOFLvEWdrROk/RJbuie/5LsfO441TK6tXYXYOFLvEWdrROk/RJbur/2sfO44M:/RrROk/OYfLEwRrROk/OfLEg
MD5:	4C2F74FBB3FF5020AEF1AC722DF8641D
SHA1:	B072CAD2913BCBD9D5BEEB3D7BB4B11D4EAC70B2
SHA-256:	5D10AD01A0944C87C2BAD937A288D00656C50AF509212FB481CE496898D3BBA5
SHA-512:	522F273DDA046744325401E79135A51467FA475567DB9D38B14A2FB8EAC5534656D623371EC21CA92FD95419EBF577CEA2C7897B5893CEB2928C879D73CE5324
Malicious:	false
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ....$ /....."#.DS.gD.$.A..~..rw.+[....!.)?..f.U..(=.=.A..Eo..... .....A..Eo.....Z.(.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..6..$ /....."#.D.1.E.$.A..~. .rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....^.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.578465633899711
Encrypted:	false
SSDEEP:	6:mmDEYOFLvEWXICQ//qVhRS1QPLr1TK6tl//MmDEYOFLvEWXIhi/HS1QPLr1TK6tT:xqTbgCPLnG/jqTKQSCPLn
MD5:	39970273A9D4707957C7BA4992E23FF2
SHA1:	A2BCD8CD07C7171EC77C36F68081D63AF0513536
SHA-256:	C79C429536A20641441CF6913BDAF190AFB3131DCF6024EF599290EFD62B39C5
SHA-512:	010D651305756B811C90B99C8A297214682FE0A93333F08C60C36147F26B68FA00DE8C1164DF9A072244F00ECDDCA29AB647E5B123762C24963C48EB35845556
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js . ...$ /....."#.D..[D.$.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....1.....0\r..m.....:. ...f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .....$ /....."#.D.(.E.$.A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....=.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.623801863535604
Encrypted:	false
SSDEEP:	6:m52YOFLvEWdMAuEhl/KzsEJ41TK6tV/l252YOFLvEWdMAuri/3EzsEJ41TK6tNt:zRMiOsD7/BRMhXsDr
MD5:	18E07072BD0176CD2A329F0A170A2D2C
SHA1:	B8F038FEB8B3B6BD85DFD1AD816D942C70E7B028
SHA-256:	F81F428C4FE9928990E207839750DDC3B6A631EECB15403408BDE2ECAA4654C7
SHA-512:	A54FF6020D4C07A0C83A2FC5BA5A2E5DEBE66C39BBCC2644E3864D3D84A4BCE8955C7C2150280BCEA3345670B4647C3C8F12265145E6460D07DE2E031DE5FF E
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .O..$ /....."#.D0.|D.$.A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.... ....#.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .....$ /....."#.D2!.E.$.A..z._a...'.v.....4p3..1.']...A..Eo..... .....A..Eo.....=i.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.572308330147026
Encrypted:	false
SSDEEP:	6:mYilPYOFLvEWd8CAdAu3dgQll/YR7BSSFong1TK6tuYilPYOFLvEWd8CAdAuEeAP:6lJR0OLBhFoM0lJRd/TTFoML
MD5:	81DE37A2C1103324E837CC8D8867C99D
SHA1:	1029866630E466210D9AE16B8C6C315D962E72DC
SHA-256:	3C50332090B76FAEBD15B20659D971BFB55CD266BD4BA7065FA6C23C25198B8D
SHA-512:	38AD4AEE9E2C4A6A203D68B16F6798ED5D98D130D4E25BE2DA61CA95D6A55BDFB2EEBEE14231E8CCF25CC705F9C8BD5BBFE0F77202E65B2AA89E4B8EA67C 59E9
Malicious:	false
Preview:	0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .8..$ /....."#.D.A}D.$.Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo.....A..Eo .....OC.....0\r..m.....R....|....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .P...$ /....."#.D...E.$.Ac}.H7M=M..-.....Ix..R.I...}Rl.$q.A..Eo..... .....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	446
Entropy (8bit):	5.600196417211991
Encrypted:	false
SSDEEP:	6:mY8nYOFLvEWdrROk/IuAe/1LVe16wG1TK6t9/EY8nYOFLvEWdrROk/IuFe/U6PvG:F8hRrROk/W+Ze2z/n8hRrROk/yPve2A
MD5:	E3B831C5AE75A86D116AE62182DB0501
SHA1:	3F608F50B6EB5B0E7DD42E23FB553B749EA80426
SHA-256:	39FA14E47616438FA94936ECEEDDE964F7B48168BB1707E115656A0D9C81A3B1
SHA-512:	114E3348E89FDB73BF26C64C099DDFE56BC972C1A4630A3BC78E64D118C032111272967CF0DD3932A381AD64646F979CED699DF2B847F022D278EA03AD8D16E
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ....$ /....."#.D..gD.$.A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....].....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js .....$ /....."#.D...E.$.A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....l.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	426
Entropy (8bit):	5.661302849717642
Encrypted:	false
SSDEEP:	6:mLrnYOFLvEWdrIoJUQXF/XzzyeqrNJIi1TK6t2LrnYOFLvEWdrIoJUQxXgQ/mqr5:ehRcSpCRrNJICAhRcGXEqrNJICzN/
MD5:	1067C246B9D7E146F0E264E5E0A8E4B4
SHA1:	A8692A54BC900965FA6DA9D8FA5471A0A95E9A4A
SHA-256:	94899653F47EC8ED4AEB15C1F3821AB8A8213CD56E0793DAFC35A2C6310A8448
SHA-512:	C2B2D0FB7912491128AD4433B2355CD06F86C3B0ECA752B1868FCA80301D5787343B7B406B142729CBDD30BC39C5BFC6DE01E30F13969C6B3FFC7E629A52E4E
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..v..$ /....."#.D3PhD.$.A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....tQ.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..<..$ /....."#.DW..E.$.A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....C.H.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.597007449533491
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhuqt/b8bLzgm2d/1TK6tkk+OEYOFLvEWdrIhuzAKt/MLCLzgm20:0Rgd8/ReERtvVRem
MD5:	2B28EE963602BA0EC9092A3BD63EC366
SHA1:	FA1ECE3FE9AC8F0D4197C74DD1C6799F1B183060
SHA-256:	491AE10A1364C60A56F28BC16FC3E719597CE0DB597B12197B293D05D88432BD
SHA-512:	7DF60B0843F11F66F6DECB2B94C647F530A58794D991BF74A6DDB3BDEA3832E84419680A6C2CC7D2E4923F6DC8EE6883B85E2FF1E87ACB2C570F386B2424ABC
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .....$ /....."#.D.@gD.$.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....D.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js .V...$ /....."#.D...E.$.AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....x.P.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	376
Entropy (8bit):	5.588423967498415
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1Kjl/jf2kx56uvp1TK6tNItMAElVYOFLvEW1KGFu/Dkx56uvp1Tq:6JJKjLswJJKGFXA
MD5:	199A995BBB3BE2BE1C10A19BB627FED1
SHA1:	2E466F21895118E8B17DC0E4EA0C7715B18531AD
SHA-256:	84346F1B75D678922A6B40A44AA1F893D15456FB33CCDCD191EEF2501F913114
SHA-512:	C90D3B242C70A00E6452F488D7944C328EA58BF9419B6AC61D4B415A073D8E4AE3EB7BFA33EF621857E6DFA94135F0E737DF214DC5F279B22BD1D522F100AD3
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .....$ /....."#.D..&D.$.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....[.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .@h..$ /....."#.D.].E.$.Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....$.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.584151760651256
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuoi/ThUDLYtmOZn1TK6tl:xRBJxDcFZLT
MD5:	4FE084007337D605202B42C4310B59BB

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0	
SHA1:	5C565424EFECCECDB7228B824AD185D25EFC1F55
SHA-256:	A492B248CD410CCA01E8706FADEFC44B6A3555D67F5CBFFC9D1B25BBDD709D61
SHA-512:	C61B1AF3DF8DADFBF8694E888FCAD0A182FD2612E08FFEA33D7C4CEFBF11DF36F4B3ED3300DBB84342A4B08BCF06424BCCB8AB2F1E3D3AA09274E1B96AAF7737
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .h...$ /....."#.DT..E.$.A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....e.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	422
Entropy (8bit):	5.601169643629143
Encrypted:	false
SSDEEP:	6:msRPYOFLvEWIa7zp7V/uVPu1TK6tQesRPYOFLvEWIa7zp78Q/akVPu1TK6tA:BPH2cgPHGkc
MD5:	367EF55EB6125193D11EAB81D2A00D52
SHA1:	F44C1A40A0007537FC69CB42BC932E2E7120766B
SHA-256:	4C908662FEF061DB5371FE4E228FA803DE4ECB28BF0EF4202717E0F00C2A2B9F
SHA-512:	DD88074EB62D151593B8CE40F45427BB8C3FF54DA76F2E36FDCFAFAED5A9A9FE6F8E80F547A8922DC72801F12D2256BF9757AD819F7772D6C7A7FE0E393098FB
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..t..$ /....."#.D.&.D.$.A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....<.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .....$ /....."#.D.7.E.$.A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....{.y.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.571219385529447
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9Qsl/zsPiM3Y1TK6t9:bJRT9NWPr0
MD5:	8EBDA043FB784A279F696FCA78CCFBCD
SHA1:	AE26F884D0183878D6CF9C99BD62EA2F47E5CA3D
SHA-256:	975F96E7815CB7C13DBBD2EC2A1C9F0A4396F956EE08B29F6D062AD2747B3867
SHA-512:	F9149DB8A35B0F5FA5D4093BA527C43232456848323368C217E80CC02F82253D488D209636B4A19DED30B02742EC5F3784E08FECE5067C46E746BEFC3FD49539
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .....$ /....."#.DB..E.$.A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	modified
Size (bytes):	208
Entropy (8bit):	5.61379031328076
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQpi/PQjBRCh/41TK6t:XRc9CQQDi/E
MD5:	91F02D0A763C31C8E69EFDBE31C3D79B
SHA1:	6BD8AB82092B1ED6E8369C55B6E502520C87BEBB
SHA-256:	F2E07554750312FF4A03D0742B3BE310FBAAA648537269FCE9128410E7DB101D
SHA-512:	FC7B83C88E9BD685A543C3BC41885E24ED0D2CC46D96E74357E6CA78170EB55908D20A8CCFE97933D128D10B4259AEC377587AAE9B35131EE735E08ED0AC00B
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js .....$ /....."#.D...F.$.APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	231

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0	
Entropy (8bit):	5.5665675349374135
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuLVt/g1ULlF4r1TK6t:bs6xRkipV6WLlF4n
MD5:	0122D8486A78A43A0F6FFA2A91C5D7DD
SHA1:	3539F6254F73187ABEF762C9C2E00333D45A7ECE
SHA-256:	F671754C2D1954935B37612016A43EC7636CB42246EFA44C60E88B65F8A89FD8
SHA-512:	DE68AC80A03B1C205F56CC6BD9C77297EC750693AF92A5A9C34C28AEFEA7D7199BF8719077FE67B7512B19E8CB23C595DE7B1C8C6C53D03C1333454B7ACF54 5
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js .....$ /....."#.D.nD.$.A.P...#4..l....5...5..).w.. .h. ~..A..Eo.....A..Eo.....w[\.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d88192ac53852604_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.493089298400675
Encrypted:	false
SSDEEP:	3:m+lPHYs8RzYOCGLvHkWBGKuKjXKXqjuSKPWFv6Al/llLYc9Lacu1isLK5m1TK5k7:mhYOFLvEWd/aFuMA//L1941TK6tDZ
MD5:	7AF35A9C668360E6E91E69734934774A
SHA1:	169F011E586437DA5803C6C78B5C88D689A4C5ED
SHA-256:	A6545F24FA0488E9A012A009A600AD3E99A31DC022694F83C3498EA0E8769232
SHA-512:	580F20FD7677BD9DD90128402A1680A34721932302ABDCA5314CDCFD71AA38CC6D39C4C80BA9507F25531DA148313365B4B903C09FF9C92999EA0CEACF2ADF D
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js .c...$ /....."#.D...E.$.A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A ..Eo.....q.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.513673234560505
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQ8//XoBMqVd3G4K41TK6trN:2DRuRXYB9Vd2kxN
MD5:	F66B198E654C3913B41E6CB0B82C2FA2
SHA1:	836A0A7D9E15463A91CEA0B07DDCC48369BC9B97
SHA-256:	3DC23BCA007CE7D09E78DF419609D841AE12960B4DDE9BB7180850896B1BD5F6
SHA-512:	2A91447AA8B24E253A03D9EE560F3787BA957EA3317DA586498389F7C8469A8C2F529CFA112D2E5780F8D32AB91B1C84CABEB8DB1C09C4982D15DF4FC15612C A
Malicious:	false
Preview:	0\r..m.....P...y.p...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .....$ /....."#.D.!.E.$.A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.. .....qGC.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.617899702570539
Encrypted:	false
SSDEEP:	6:mkqYOFLvEWd8CAd9Qfv/l/EMmuA424r1TK6t4kqYOFLvEWd8CAd9QU/WGtuA424v:+RQGv//rnSRQfcrn
MD5:	CC7581EED2217FAF0973E227BFB0B3E2
SHA1:	604D77084E0561204951ABD906EF79F301090EB3
SHA-256:	33F3EA8922C8C2E38B6A4DB23808FD603BC913C1170073F09314E36C75E4172E
SHA-512:	25EFD2A2E5FFFFF1516F22B2B5E1CC9ECB9EF79E6D8D238E608B420E7E72FA63C48EFA4EAD5231F21F6AF85ECB35553ABDA7266435F9EF4A9C9B9CD89530CE 18
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .+...$ /....."#.D.k.D.$.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo... .....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js .?...$ /....."#.D...F.$.A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo..... .....A..Eo.....ZQb?.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f4a0d4ca2f3b95da_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.493227920729181
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAuPGBwl/KyC8n1TK6tnl:xhRTNGB17Qh
MD5:	09DCAF21010167505921BFD9BE9706C1
SHA1:	A788DE4F203E62D5843604C23A110667C569AD68
SHA-256:	55F5190C725642C94DE9AD1E9ED43DAB403ED25A14A713E22EF3F6C521999F13
SHA-512:	14835763288DFC82976E459DB4FBD4775D3987C9C457D13AA480F1B46A0DDFB8A036DA7BC3DAA21F8BF12CF362B27C0F0FC79CDFE8C167616FC331546EB592
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .....$ /....."#.D...E.$.A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....1.. .....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	442
Entropy (8bit):	5.619772709138325
Encrypted:	false
SSDEEP:	6:mQZYOFLvEWdrROk/VQK/9zDLmB41TK6tB+QZYOFLvEWdrROk/VQW/7pLmB41TK6P:nRrROk/Vzz+mzRrROk/VSmNt
MD5:	81A4584CFBE29DD2824281AA3981DBF8
SHA1:	FEF7AAB2A0B33E99F611209FF8D43564D901BF66
SHA-256:	F49539516631BCDE41D06A3CE8330EBA55217754F0DA51FEFFBA9DA143DEDD24
SHA-512:	B2EE7882DFE0C5E82A08265CC5F3DDD9D11458196A422E34CC376B2BD8DC7EDE7B8E886B4714B3405FC68BA790FCA2E08D2689BE7CE8AAA9772F83F0A9264(09
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js ..}..$ /....."#.DI0lD.$.A ./.ev.....N~..6.b.....$.j;:C...A..Eo..... .....A..Eo.....=.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .,l..$ /....."#.D...E.$.A ./.ev.....N~..6. b.....$.j;:C...A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.545992563975379
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuXq/LYGAdm9741TK6tUF:qxRcVuAdu7E2F
MD5:	A8C3A23F01B78EEFDF38EE20BF8D2748
SHA1:	919B4D6D43AFB8187BC7855F0D76494ED1E2C76F
SHA-256:	0A519AC0A158580E8C65ACC87BA1C4E0B1A5A973A0F915C4BBADB4F5924AE39D
SHA-512:	209F2D77B859E3C77D674C432877768884B1599785FC20B820A6E0FA6F3BD8E0E8731CB2271C2664427C35CDADBB75EAF1F3D4DCEE4E849A127AB29814D3F9E
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js ..}..$ /....."#.Dn..E.$.A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..E o.....+.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.511417306471299
Encrypted:	false
SSDEEP:	3:m+lUg18RzYOCGLvHkWBGKuKjXKrAUWiKPWFvUABwlllllmSB6shoq+Nem1TK5kt/:mMOYOFLvEWdwAPVupQll/lkJn1TK6t
MD5:	BC48DA4BCF0EFE5885D2B8C142B72E23
SHA1:	1C88A1413D37FE35C0A1EDF8184CA84DAFC943F7
SHA-256:	B0E47E2B0541C4C240A3629276B8BF4F026C634A2CED2D817709EDD6B0EEEF84
SHA-512:	1146997D661421076F58BB1E1E6E3E7A7B245BB7239D416DFC1E5C1C0B8AC3B76702B0E3B8C0CF054835C885178823198B987AE21F516E13F77D7672DEBBF0F8
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0	
Preview:	0\r..m.....L....Ey...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .....$ /....."#.D...E.$.A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....a.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fdd733564de6fbcb_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.589163482503573
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQ5/07fzhcsBXIh1TK6tW:mxRBJQx7fDB0
MD5:	DA0676EFF7772A219800B3A9B6F2550B
SHA1:	005626E36AE3BC09D01006E2C69C1E87C709DEA0
SHA-256:	B7D5BC92517C72BEEECC5F1F0862951B2049B7AD7FFAF1C97F214DF2F2C6A58B
SHA-512:	7635AF35EAAF19CFA85B940BD3D97040733FCD5B170F42224F6745F2FF09A5D4C8E04B9B364F782550C9CF6928DD712B900B239C9EFF91E889081852A6B2A8EA
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .?L..$ /....."#.D(e.E.$.A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....".O.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	456
Entropy (8bit):	5.561533995405289
Encrypted:	false
SSDEEP:	6:msPYOFLvEWdrROk/RJUQti/Hsc3Me/1TK6th98sPYOFLvEWdrROk/RJUQ/QQ/Z4x:3RrROk/sW0sc39FRrROk/sR5cU
MD5:	3D2CDAC997DB8719B93A37478AEBB43D
SHA1:	820F0EA451AAB0651C414ADB3AAFF36826A6FCF5
SHA-256:	8925B1D4F35D91D7E71B280D1707D641E454C2D524913FB630F4092B700875D9
SHA-512:	B190C4A62EC79DE5371BD61FD9126F5C9CA129D385A8DD73DD1C4EC4151458E4637733984C97C27C356CB96CD6A8FDEF4F0E4630B9EFC4EAF9938D89EA612E8
Malicious:	false
Preview:	0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js ....$ /....."#.D%"nD.$.A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....0\r..m.....d...<.s...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .Cr..$ /....."#.D..E.$.A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....tVa.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	2016
Entropy (8bit):	5.289962133883376
Encrypted:	false
SSDEEP:	24:0I2bYdB8J6MbkeljKqRom9cbSZYdD1HBGxGMANi1zrcSqc088I7bWQi2QXN89c6L:t2kdhMkCqm9cbSW1HGxGHiFc4ap22Zg
MD5:	C4E6F9B3C9FD5306AFA5DFB7E2F892D5
SHA1:	1844737CF1D833F45D499AA8FFB559391EE89E89
SHA-256:	FD39D1ABCDF10053EFE20C54439BF389157C1E0A259015061D96600E3CCA204D
SHA-512:	725BCE6AC5B367BD39BC0812CFC6BA2AB9B6DC97A231ECF81F89B7879890C6B51A52B5A1FEB6292F731CFAD070F6946D5AAC834B4FA4B9FDC601A5DB9D92609
Malicious:	false
Preview:	.....goy retne....'.....'.....:.y~A.@.....*..@.....oB*.....#...(@.....k7A.@.....D.4.@.....[.i..%.@.....<...W..J..... ..,+..._.#@.....J..j...@.....6<|.....A?.2:..@.....+.{..'@.....*)....J:@.....2q....@.....P....V@.....+.U.!..V@.....P[. q@... .....!...0.o@.....u\]..q@.....@.....*....@.....o..k..@.....^.~..z.@.....o.@.....Gy.'.h.@.....F..=z;.@.....3...@..... .....v...q..@.....C..M..@.....a.....~.,.4>.@.....&.S....@.....@..x.@.....=....m..@.....:/...@.....q.@.....MV3..@. .....:..N.A..@.....Z.....4.P.oy retne

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	294
Entropy (8bit):	5.159390950412661
Encrypted:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG	
SSDEEP:	6:mVjyq2P92nKuAl9OmbnIFUtpneGr1ZmwPNm9RkwO92nKuAl9OmbjLJ:Jv4HAahFUtpe81/PY5LHAaSJ
MD5:	7A28ACB59F70CF20953E0A4AA6CDD103
SHA1:	1B80619F477F2C33FC39DC66705856B58B431D5A
SHA-256:	8B7D45694EBD5B707B5B96D743F9F8758A02EA9AC26824B476E1A9B5B96536FE
SHA-512:	9776B1D1E871A14C9BAF0B63040F02CB8C38C9A1EB1D4064FD937A666F670FFED1668925FF7A5EEEF0F5332F67507F5FC5EF5BFC4E5F7F678E1F4D94CC31CFEC
Malicious:	false
Preview:	2021/05/04-21:37:37.221 1bc0 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/05/04-21:37:37.224 1bc0 Recovering log #3.2021/05/04-21:37:37.225 1bc0 Reusing old log C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/000003.log .

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Visited Links	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	917504
Entropy (8bit):	0.007909552735237937
Encrypted:	false
SSDEEP:	12:I+1rDro+1rDro+1rDrolfrgrocrgAmJocrgAmJocrgAmJ:T13rz13rz13r+fUrjUVJjUVJjUVJ
MD5:	28C3F901AA5AC270CCAB75AA191F3258
SHA1:	5D399FD68F093714478F4E722E6432F2F242EC89
SHA-256:	7C8E9508FC031C0B9B0EF7AA2AC874A1C14DE506A9AA035917F03E6CA1D3480D
SHA-512:	FE180F9F8D19E668F38B787F02BA2E6871EB3B9D90BD1CB9AAC9FFBCECD2EEB1F21EE16C422994B096BE8AEAF8E05CDB4653B9DD023B9DAA8C7C870706E1E925
Malicious:	false
Preview:	VLnk.....?.....+.}.^1..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210505043724Z-239.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 107 x -152 x 32
Category:	dropped
Size (bytes):	65110
Entropy (8bit):	2.1152568299519108
Encrypted:	false
SSDEEP:	48:55i5Bw6J8J86DEUcZpLqy7PFqm7ZZq8bNqbg5L6bvObiMPju3:fIBw6J8J86shLq3
MD5:	C2806B0C2398F311842C4FE04D6F5DC6
SHA1:	1FB409CAB558C07CCB9753AD8301E98012FEB9A7
SHA-256:	7F4E880D8182CBCC060227B4E916411EE670BFDF9538552E8B82C17B2C92C348
SHA-512:	7E37ADC5CF8E6A2BCB0CC1B5CB1954EA85CABFAAC6DAF826936A1E7326425273BAA868DCB16C3F63108B3B5D2274FEE833AC8201F50B62EC41AAB382452B97A6
Malicious:	false
Preview:	BMV.....6...(...k...h.... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3024000
Category:	modified
Size (bytes):	32768
Entropy (8bit):	3.3873623622141498
Encrypted:	false
SSDEEP:	96:iR49IVXEBodRBkQeOhFVCsL49IVXEBodRBkRxeOhAVCs749IVXEBodRBklxeOhTf:iGedRBCedRBWedRB3edRBr
MD5:	3828B7C42E233B119D0853817DAA07D7
SHA1:	4F414C0F0257C137623BDAFBD3CB0B55C7FA0CF0
SHA-256:	FD8979D317C5392CF5BA95E09B25528D7383F55E925D30827AE623CA178D8951
SHA-512:	B01CE61FED7BE1FEBE8D7865D94E1092DA3BCE16ED80EFB5B1460E1A56A027D9778A9B14DE931ACB2F36E85FA572F19453B7715ADFC00D332891C551DCE6971A
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages	
Preview:	SQLite format 3.....@ .....$.....1.....T...U.1.D..... ....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	34928
Entropy (8bit):	3.2002425304549593
Encrypted:	false
SSDEEP:	96:M7OhFVCPE949IVXEBodRBk4eOhFVCsBLR49IVXEBodRBkGxeOhAVCsdd49IVXEBn:MAiedRBzLGedRB8CedRB9yedRBs
MD5:	37C6F0FFB4BC6BFEF158349C66FE2F02
SHA1:	BF9E09B3623B439B0A8F2484E321562B65DF0614
SHA-256:	09CB1487A80CD0EAE68B0F68D864B5AA6538F892FB4AB260002F27C91BCC7F1C
SHA-512:	1978E6A22B7EEB063CCFB4AF0DCD7F15116FF6876E587DD562EFD01F8915D0B25DD282F505E236C9AA3C26766BFFE95C6AAF8271ACD22CFE67E9A7C57EAAB67
Malicious:	false
Preview:	.....gn'^..... .....X.. .h...y..... .....

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\UserCache.bin	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	data
Category:	dropped
Size (bytes):	63598
Entropy (8bit):	5.433041226997456
Encrypted:	false
SSDEEP:	768:PCbGNFYGpiyVFiCUZcdeL6f3Tr6BfvCHIlsuO4nbcyYyu:J0GpiyVFiBcYL6f3TuXCoHJK
MD5:	B49FE17CE6BBCD288BFE9E9E8CDF92D6
SHA1:	DBB11DE534670C182E0197D40CA763D2A9969FEA
SHA-256:	00F27048CB927B07E2CE208A00131872C467B127860FAF61E08D1B26E5EF8280
SHA-512:	3A588D6594F79EFB9D7B46F5A32BD6A27B5636DFC9C0E2DF0DA34827EEB46C36A18E569729D68DE0A84C07167E60785B282096016343C783F9792CFEDEF3D01
Malicious:	false
Preview:	4.382.88.FID.2:o:.....:F:AgencyFB-Reg.P:Agency FB.L:$....."F:Agency FB.#.94.FID.2:o:.....:F:AgencyFB-Bold.P:Agency FB Bold.L:%....." F:Agency FB.#.82.FID.2:o:.....:F:Algerian.P:Algerian.L:$.....RF:Algerian.#.93.FID.2:o:.....:F:ArialNarrow.P:Arial Narrow.L:$....."F:Arial Narrow.#.107.FID.2:o:.....:F:ArialNarrow-Italic.P:Arial Narrow Italic.L:$....."F:Arial Narrow.#.103.FID.2:o:.....:F:ArialNarrow-Bold.P:Arial Narrow Bold.L:%..... ....."F:Arial Narrow.#.116.FID.2:o:.....:F:ArialNarrow-BoldItalic.P:Arial Narrow Bold Italic.L:%....."F:Arial Narrow.#.75.FID.2:o:.....:F:ArialMT.P:Arial.L:$....."F:Arial.#.89.FID.2:o:.....:F:Arial-ItalicMT.P:Arial Italic.L:$....."F:Arial.#.85.FID.2:o:.....:F:Arial-BoldMT.P:Arial Bold.L:$..... "F:Arial.#.98.FID.2:o:.....:F:Arial-B

C:\Users\user\AppData\Local\Google\Chrome\User Data\09e82636-9696-4c70-b4c9-0c4353bce75e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7489562423803466
Encrypted:	false
SSDEEP:	384:RHdySsPZkvMSVn521NKr/v+G3tGkZH0tGRYrzQSUxb5IIQbrD6xmvUzgq2WVOgE2:d6mRxCEF9Qef8u0s/DWmKs2WBR
MD5:	9D9EE2D847A0307EF735D63C40FB9D46
SHA1:	214019E8B1E69BA7215D57653AB56BE06231536D
SHA-256:	776F91663D6E6249B662647D60A1996A21CCFC68BDF3F12A9219F686CD0912D0
SHA-512:	E48DDAB8AC51B0000BBF241D47BE2060D9952BF5B5E6E9D4B6C430934E7ACDEC8B391F14155221B8E91D8ABC1EF06F448E24512D2470915C7AFE435318B63C3
Malicious:	false
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....98.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\0b0adde5-de30-44e9-bafb-8a74599a27a7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\0b0adde5-de30-44e9-bafb-8a74599a27a7.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	362936
Entropy (8bit):	6.028181733871655
Encrypted:	false
SSDEEP:	6144:WEr/NOXs8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBA:d7NOxxzurRDn9nfNxF4ijZVtilBA
MD5:	2CA046A323FCC5AF5C58CA940291F1FE
SHA1:	C6C61E7C79EF474A68256C8B1572ACE2A89DFD51
SHA-256:	2C5099FEAE1F7150B7A3B935140A5E4902F2D199E511DB4D49B151D75B4F8093
SHA-512:	4D4B3F63F8DF762285C5BCC27AFBECCB236B0578D0E2FF3B9E6FF772BA40DF256458E128370B26809132BE082F4156934DC82608C5DDF753903F016DAD0AD15
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":1.620189504525977e+12,"network":1.620157107e+12,"ticks":181522551.0,"uncertainty":4884260.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075120998"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\173bf113-f70c-4cc0-858f-826f0b8bcd24.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):	362842
Entropy (8bit):	6.027999935623232
Encrypted:	false
SSDEEP:	6144:OEr/NOXs8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBA:V7NOxxzurRDn9nfNxF4ijZVtilBA
MD5:	C16A7107D1E5ACAA31D39EE76DB57DBA
SHA1:	FAADB117817F321FAB7DBAD4A829D1E93EBE4C7B
SHA-256:	2DC30FDA58DF3AC5ECA5C8D4090CCF06B4B53D29BAA7B72B8DF0FC0FDA0394A0
SHA-512:	206CEE8677EAC18184F626689E0EE4496B0769F58A2AF8B741BDCCB3E6AE9B0D4DEBD050616CE5E331A4C0BAAA8E40225722B0A0415447CB4EA73DAB3938A8C5
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":1.620189504525977e+12,"network":1.620157107e+12,"ticks":181522551.0,"uncertainty":4884260.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075120998"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\28f96999-f0e3-4f35-a80f-d61de713d891.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7489200208885074
Encrypted:	false
SSDEEP:	384:BHdySsPZkvMSVn521NKr/v+G3tGkZH0tGRYrzQSUxb5IIQbrD6xmvbpzgq2WVOgF:t6mRxCE89Qef8u0s/DWmKs2WBJ
MD5:	ABA8C108ED3459E556FE087A4A4998B6
SHA1:	70917A83147F261CA831FBBB77EA02C444EBEC53
SHA-256:	DF6B40775F62FCE5DC245DAB2586A4F32C72222B86DFF59AF6845B0009B430A9
SHA-512:	D6E8FD3A67060D855AFAD81F4B69EA3DE8E137123DA1C95D903A664AA59C57A0B684FF1A9F1037AB031B1ADB037078E35108505A2EC7E781575B197FF7D2500
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....98.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\4a487a11-82d5-4769-825f-bb955ad785ed.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):	359271
Entropy (8bit):	6.0154296632329665

C:\Users\user\AppData\Local\Google\Chrome\User Data\4a487a11-82d5-4769-825f-bb955ad785ed.tmp	
Encrypted:	false
SSDEEP:	6144:dEr/NOXs8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBA:C7NOxxzurRDn9nfNxF4ijZVtilBA
MD5:	C4B33A3459D1B0EC724CFB2D8823E64E
SHA1:	019EC3E8504302E0951163059C80287024796CB6
SHA-256:	1ABD51E59C2745B1FEA038B4ED55CD61D28A472E12AF6A4334286100C9ADE2FD
SHA-512:	F0FDB68ACC0BAFEF225C9E2A3971900FED23F15230E0661B0E731205161FB3A0336274F645AAC5C890426EAC978C3464F18FE44E6DEDBDF22CA6945A5D55394
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":1.620189504525977e+12,"network":1.620157107e+12,"ticks":181522551.0,"uncertainty":4884260.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMlXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075120998"},"policy":{"last_statistics_update":"13264663101006

C:\Users\user\AppData\Local\Google\Chrome\User Data\6a3f39b5-eec4-4f67-9165-1d24ee68ef19.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.748556024810905
Encrypted:	false
SSDEEP:	384:nHdySsPZYMb21NKr/v+G3tGkZH0tGRYrzQSUxb5lIQbrD6xmvUzgq2WVOgEmNQS/:PmRxCEF9Qef8u0s/DWmKs2WBL
MD5:	4BB4A1B85D00742D58934905D3FA11C1
SHA1:	A6355E3D9278B1855ABC50C4B24CFB7F8B36B4F9
SHA-256:	E59FF1504F8CF195B712FB313A7441887A5A18723896A4C1D34551F0E022BA74
SHA-512:	D45DFC8C9F92D5DD41A6180B86D2F90AD70BEB1D0A4DDF8C2B22DA2A9EEE9EFFAABA81FB1CB5B856B79E52592398D36CC08AE1E068B8C402062AEA5378A0C64
Malicious:	false
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....98.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\8d69a971-6cf3-4978-87be-562abc79c264.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):	362842
Entropy (8bit):	6.027999935623232
Encrypted:	false
SSDEEP:	6144:OEr/NOXs8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBA:V7NOxxzurRDn9nfNxF4ijZVtilBA
MD5:	C16A7107D1E5ACAA31D39EE76DB57DBA
SHA1:	FAADB117817F321FAB7DBAD4A829D1E93EBE4C7B
SHA-256:	2DC30FDA58DF3AC5ECA5C8D4090CCF06B4B53D29BAA7B72B8DF0FC0FDA0394A0
SHA-512:	206CEE8677EAC18184F626689E0EE4496B0769F58A2AF8B741BDCCB3E6AE9B0D4DEBD050616CE5E331A4C0BAAA8E40225722B0A0415447CB4EA73DAB3938A8C5
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":1.620189504525977e+12,"network":1.620157107e+12,"ticks":181522551.0,"uncertainty":4884260.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMlXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075120998"},"plugins":{"metadata":{"adobe-flash-player":{"disp

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):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9iTXYDu6cR9iTXYDu6cR9n:+Y66cR4TXY66cR4TXY66cR9
MD5:	569FA64ACAA310B1DE1A6250CC7356B0
SHA1:	14251450C245F8612958BF94779E8B72AE6D6213

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
SHA-256:	AEE20ADEBF2D35EB8A39BE2DC391B0E5966EFCB4AFDC971BB3A18115C929F563
SHA-512:	850914A053EF541046B29260266C17FEFF2466A87784394F9AB3B565D2EA1E656F61F02BDB78F9F9676E90365F837F3709BCC0856B3B844256848F477250E0C7
Malicious:	false
Preview:	sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.sdPC.....8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1704ca54-9349-4cf0-ac97-9bff9f5ae3ef.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):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1984a2dc-ae2c-47d2-b86b-1bc5989b41e2.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):	16745
Entropy (8bit):	5.577215528253041
Encrypted:	false
SSDEEP:	384:xoR3tTLlNWX01kXqKf/pUZNCgVLH2HfDkrUArmkt4L:6Llu01kXqKf/pUZNCgVLH2HfgrUAjtQ
MD5:	19F8614143649B9130190C32DD755010
SHA1:	ACEE0509D17EDFEB69BB6D1F472ED5673AC6FA2B
SHA-256:	A5B03875366D128D55E39F11302E2F1305647B06D923F93F42295EE449A52F30
SHA-512:	528D5C839213AE19B999939C19C7E2972FD43B745D0DA0C784CBB93F00C93C7D2C2D498B53F5B7459F9C2A1DC55D85CBDC016DDE74E84ACD108D7CFFE50C53B
Malicious:	false
Preview:	{"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":"13264663101145506","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_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\22bba30f-fe97-4eab-abbd-83dfa1a134ca.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):	22596
Entropy (8bit):	5.535873426089377
Encrypted:	false
SSDEEP:	384:xoR3tuLlNWX01kXqKf/pUZNCgVLH2HfDkrUZHGLnTEm1it4Ln:hLlu01kXqKf/pUZNCgVLH2HfgrU9GLnn
MD5:	45992FEFE6248B62934324C01004E325
SHA1:	39BBCBBCE7AA1E1FD6874027F2CF978E21E6A69F
SHA-256:	3014F3F90DCCC022A1C00CB8C1CE29ABD4108AD20E018CDD224F1817E471D18F
SHA-512:	E9529A9734CE16E0BB437F9A7130AE8E4A92B96C73190413B7D4DDF0A7BD86DCADF9A7D3B142EB512B8886E45BE0BE06183D8C5583C5F3389245B7F392C4891A
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\22bba30f-fe97-4eab-abbd-83dfa1a134ca.tmp

Preview:	{"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":"13264663101145506","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_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3fc9083a-031d-414a-8ca4-0b0c0ec65718.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):	5709
Entropy (8bit):	5.186489807907654
Encrypted:	false
SSDEEP:	96:nGrF85lnfVup7uSVOJIk0JCKL8xkP11CybOTQVuwn:nGrefV5SqC4KWkPP
MD5:	E449FE2B83C569E0376ABDDAA623E168
SHA1:	4D8687538C0FE7AB409A734A5CA9B13F7D1E5594
SHA-256:	63658D1563C432148CA8ADD044056C51304E06E7CD6FD6691C31D493834984B3
SHA-512:	EF0B8F885331BD97D696513CF943795135FA87F51274F19F6A7408A974703234A140E19B559878B85A7BC5A630B4F3D49D7B27C5ECC3D4DE0BD33F3AD2DE03F3
Malicious:	false
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264663101436525","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4a93eb66-30ba-4de3-8ea0-312ddb38039b.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):	2235
Entropy (8bit):	4.901730162778734
Encrypted:	false
SSDEEP:	48:Y2n6qtwTCXDHz5swRLssATsbr6p1sryKsb3zsWMH3YhbxD:JnxOTCXDHzDYc6pEO/GohVD
MD5:	194340CBBD0072F2ECDB85242F9DC73D
SHA1:	55A50767056E0DCB81D2C08143F32519248A1525
SHA-256:	9C840B1F390A130DE1FE82170583EA0609701122357225880AF42542206AD16C
SHA-512:	857C09C136B7CF60EC136A3F2E5D0343B2D925E6AACAC800DCA9C2CAD73A54521C9F4BE3C39757E9899D245FA277FAA9CBA6F1E215458A44C29D5B97150C16 7
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.google.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267255106266119","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267255106345464","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8ec71e31-c09d-44e3-9325-61cdb8256334.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.221496184163148
Encrypted:	false
SSDEEP:	6:mTOAq2P923iKKdK9RXXTZIFUtpeqZmwPet7kwO923iKKdK9RXX5LJ:qv45Kk7XT2FUtpP/PG75L5Kk7XVJ
MD5:	CB6F794EBE68DEAAFF2C09B818A0583C
SHA1:	A9C356FD3410C44984979FB712765EE1536C1A22
SHA-256:	1275286A72FF5474D3C5F1B1C0958771B3D60F4B6C666791786D6D08E83B2540
SHA-512:	DA0F5350AEC7D627A680026470BED27A612ED57184AAE45119450FE002764F9B1CF31D972DA1E1D120D6CB0E1D1D276AAB9D451F26662F187FAD29885945C7C
Malicious:	false
Preview:	2021/05/04-21:38:35.419 1840 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/05/04-21:38:35.468 1840 Recovering log #3.2021/05/04-21:38:35.478 1840 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.188247620292106
Encrypted:	false
SSDEEP:	6:mTXOq2P923iKKdKyDZIFUtpebxhZmwPebakwO923iKKdKyJLJ:+Ov45Kk02FUtpih/P55L5KkWJ
MD5:	C8C19CC51BAC370A1F7969CC7D2F680B
SHA1:	078B9E8C5AED7D32F0EB2F7D0942A40EA17BE3B3
SHA-256:	ACA33F8B27FC3197DA9FA3013708AF9C15525EEF3C08C60AFEF65EF1D76DF24C
SHA-512:	FE436E2F95DFB7B0605E334B79F3C8AA61E9942F08FB4D4E73330B1601657091F621BA9CC8D8EB1F4E2E92D1811AC508E27700F69AB69CC2792754CD00ADEE6
Malicious:	false
Preview:	2021/05/04-21:38:35.346 1840 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/05/04-21:38:35.351 1840 Recovering log #3.2021/05/04-21:38:35.352 1840 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	1.3006771036344906
Encrypted:	false
SSDEEP:	24:TLyqJLbXaFpEO5bNmISHn06UwV/q9xqa0ZbOEikr7D0rzPS:TekLLOpEO5J/Kn7Uyq9xWZb2kn
MD5:	4D1388A02CCC5EC5DD3CAF5632A1ECAC
SHA1:	D1BB41B6D1A92CD76AECED42550604A1B058FB03
SHA-256:	845440E197FE113A6E2248A01C4200708A915F4060F5580B3D080D977F122D5F
SHA-512:	9D8E901A4508BFE617A35D725655A315DC2119B97FC9D397D9C5220B2D1871E2387F5258C3F60556AF65D4D80356F604507A2531F25CCDFC6FB4C99C9963CCF
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9695656481849182
Encrypted:	false
SSDEEP:	24:BIL4rtEy8WRqLbJLbXaFpEO5bNmISHn06UwK8:BI+7q5LLOpEO5J/Kn7U58
MD5:	CB850731F58D110D3601BB0274D58807
SHA1:	8FF1CED0415560BFF1019B1E8392445B7D843A05
SHA-256:	DA35BB58CEB999C56DCF986295FC624399C49602239E803AF1A0C6277FE5ED8D
SHA-512:	8A2632CDC8F0A99264D15EDCE725D121F5D260187DB9B0E32EB83490802D29C6B10F0A3C18D79DB68D56FD2895C43C4CB295DE94798AD81A1102F29D87D6FD
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Preview:	.....W..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1143
Entropy (8bit):	3.511622682669762
Encrypted:	false
SSDEEP:	24:34Sun/83ylrlCJc0kVxMPX/7Ee+uL4z0QMexEMP6lLlr:34vnkGxec0kwPX/p+a4zPTPORr
MD5:	65CAD1DE2494E106DE8625DCFFBE212B
SHA1:	2964CD0579B1A4EB52C9CB754FA9CED3949E3323
SHA-256:	4411ACF800B988497CE0B0C29C25C304E7E28FE95ED3C75EFFF2AEEFDBA25CEF
SHA-512:	00BE899BCF15C0743BC49AAC0E84353E374593BB0AE819867FD9E477A2494D1046A96F72C3100040C4AA840F84C4AA5BBFD94C0EB3DB778FED21F525CE4E70E 6
Malicious:	false
Preview:	SNSS.....!.....1..,.....$...f0f9d329_37c1_44f9_9b8c_fae89f394cdc.....B..... .....5..0.....&...{2F4F8386-A58B-4B0C-A17B-2FAAF764E551}.....E...https://traffking.ru/square?utm_term=reflective+practice+template+ nhs.....h.....`.....5.....6.....8.....P.....P.....E...h.t.t.p.s.:./.r.a.f.f.k.i.n.g...r.u./.s.q.u.a.r.e.?. u.t.m._.t.e.r.m.=.r.e.f.l.e.c.t.i.v.e.+.p.r.a.c.t.i.c.e.+.t.e.m.p.l.a.t.e.+.n.h.s.....8.....0.....8.....?..... ....null.....E...https://traffking.ru/square?utm_term=reflective+pract

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	183
Entropy (8bit):	4.267376444120917
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+GgGg:qT5z/t2qoEwhXeLKBt
MD5:	7FA0F874EABF1EED31988230680AD210
SHA1:	E71B360F1E8D5C278A051AD03DFB9027ACCF38C3
SHA-256:	09E15F8939364145E710C314EBD93FD19BF60C2B6B20BF8023315D617B6B141B
SHA-512:	AF4C2E595AA0B1FD96474A0E73530B38BE5F2906B10BE1DEFC0A9221129A3E5BB8D0816777550863AD426C5C836ECA1F0C384986C2A1108E2E4CA20EF10A782
Malicious:	false
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.204483480296538
Encrypted:	false
SSDEEP:	6:mT4l+q2P923iKKdK8aPrqIFUtpe4UZmwPe40VkwO923iKKdK8amLJ:Sv45KkL3FUtpK/P25L5KkQJ
MD5:	B19B5671F8D1A1E56F9C9649C4D119D3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
SHA1:	F8C24F1E18D7616CD7CD26880DF1CFED4B165F7B
SHA-256:	9A5926CBD53207DCA86B1B2B881C6DBF884E8054FB1E3F791BF1525BC228E02C
SHA-512:	63518826A0EA578DC911D4513618546CA4C4F2FD7BC7A986ED3B2E72F7E5BA75A1651EF0D2F8D7D72FA575BB905B27656AB0AC734EE9EF8D6D744839226588A
Malicious:	false
Preview:	2021/05/04-21:38:21.461 16d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/05/04-21:38:21.462 16d8 Recovering log #3.2021/05/04-21:38:21.462 16d8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	627
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	12:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW:
MD5:	9D7435EA49A80FDD66E4915F513017F9
SHA1:	469F6C6E4B19B85CC1BE497812B2F20864F4FF2C
SHA-256:	409D4C47E940688527D730B996E8991E010988C7671565467ED69D640D0947F3
SHA-512:	0561CD632D4219AEF4686DE40EC092921384CA89755D354801E0EAEC8645A8630A180807AF518AC8FCF01F71EB3D10FAA9CE1E62C7A7226A274975BDCB7EEB4C
Malicious:	false
Preview:	.f.5..............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.189030036236107
Encrypted:	false
SSDEEP:	6:mTSq2P923iKKdK8NIFUtpexFa9ZmwPeDRFkwO923iKKdK8+eLJ:vv45KkpFUtp3/Ps5L5KkqJ
MD5:	D3B19CE65E9C83E417D9CEB1C2FC0A86
SHA1:	E0F56FAA6620997E38311F49492AC27E652A659C
SHA-256:	769425B8BB9CA58CB67C270D1EDE34EA33175380BAAE301ED607809BC4DE81FA
SHA-512:	482CB1A75ABE3BECB247712D4CE63BB05C6CCAEABDD87A0C09B8A2B1EE39BAA783A35FA4B419DCB2C7FC9087D76518C52DE8CE0256083F1B428FBA231550E4DB
Malicious:	false
Preview:	2021/05/04-21:38:23.815 1514 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/05/04-21:38:23.816 1514 Recovering log #3.2021/05/04-21:38:23.817 1514 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0lTpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_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):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","hqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","L

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):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Preview:	.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):	374
Entropy (8bit):	5.220401544194585
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
SSDEEP:	6:mToq2P923iKKdK25+Xqx8chI+IFUtpeZ1ZmwPeRkwO923iKKdK25+Xqx8ch+/WLJ:hv45KkTXfchI3FUtpW/Pu5L5KkTXfchn
MD5:	C1CFDE34205758F06E1FCAA2C3A7B30A
SHA1:	F9CA7B66E8A0CEB685AFB8D0B00086F8C8746AA7
SHA-256:	9910CE66ED9993D0FA6E4B73DB125F368D2184C59FC62998D819331E7BC796A5
SHA-512:	413CA27F3E93295299C2B6EA71B3A2C9EE1B7F363353E80B24173FF06AB753C5050F4C26296133C8012265653F2ADAE9F77C33A5DCEBF6763A0C11725BA025F4
Malicious:	false
Preview:	2021/05/04-21:38:35.300 1840 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/05/04-21:38:35.302 1840 Recovering log #3.2021/05/04-21:38:35.306 1840 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\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	360
Entropy (8bit):	5.230772925665142
Encrypted:	false
SSDEEP:	6:mTjUq2P923iKKdK25+XuoIFUtpetFUdzZmwPexkwO923iKKdK25+XuxWLJ:tv45KkTXYFUtp6U1/PS5L5KkTXHJ
MD5:	89F9AF7B35C53B88B74390E43F092686
SHA1:	77F8E4DF22E096306E5CFEB4D9C90458F2D8CA9B
SHA-256:	BC524A0D4D82F02604B175CCF219BC910AA13865DBF19673416630BB5BAF9F8D
SHA-512:	148787DCF29E1D065909F842C5118571A30CD69C6F2595E4D32B98B0B65724AA2632155628D0BCCE72132394C90B360D6AD8DEC9D1E1BFE8336EE700D6DBC55
Malicious:	false
Preview:	2021/05/04-21:38:35.267 1840 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/05/04-21:38:35.268 1840 Recovering log #3.2021/05/04-21:38:35.269 1840 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.216624366369379
Encrypted:	false
SSDEEP:	6:mTmDq2P923iKKdKWT5g1IdqIFUtpeJZmwPe17kwO923iKKdKWT5g1I3ULJ:JDv45Kkg5gSRFUtp8/PC5L5Kkg5gS3SJ
MD5:	8F2B9EB9AF84854CD7CECDDD040D9A3B
SHA1:	C1318480EC4BDCB25B4B26CB8AB1848369B7CE1D
SHA-256:	3D2B9ADFF6B582EB798C31AB300C22BD9E503DDEA5F760D9CC5D815A593FD4F5
SHA-512:	5AAF0ABA8FB1BE898F4079DBAA63CEFE78DF12BE282B25582BB26603EE59795A3A6A47B4E31D96D6980AE796193D464B1AB5AB4869D47BE2F24AA9EFCEE1F5EE
Malicious:	false
Preview:	2021/05/04-21:38:35.186 1840 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/05/04-21:38:35.209 1840 Recovering log #3.2021/05/04-21:38:35.210 1840 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8720
Entropy (8bit):	0.21916490374438005
Encrypted:	false
SSDEEP:	3:mPlilln3lljq7A/mhWJFuQ3yy7IOWUKBll9ol/dweytllrE9SFcTp4AGZVV9RUA:mPlSs75fOe4/d0Xi99pG/3
MD5:	C65A01A39B268F57BEF17B80CF55822B
SHA1:	4E428B83731C36AC848E71F02101191516218C1F
SHA-256:	A43F614E3B7ADFAA80C764E77EBE543B8B05959F0DD8511E7085A2B3B77F2A88
SHA-512:	DB965E07ADECF6A2B4A47786E78ED5AE94E5A2A7D89A3364C2AF74FCC6E51A22A7CD4DD439ED5D58D7ED5DC841025DAC328E48513F04363930E76F6C41E6195
Malicious:	false
Preview:	...../.#..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	5.475654169114387
Encrypted:	false
SSDEEP:	48:bc4GXAwYLa7dLMh+8dbJV5spByLbQSefgGsNrS0U9RdiN9e:YThYLa7dLMhVdbJV5SByLbQ5fgGsrS0A
MD5:	5536E123249BFCEFA607D8D2E411C8BA
SHA1:	DC36B16A74449EDED022EE142A59E1D827E7B568
SHA-256:	32791262754DEDC51A0F3C074F716A8882DF12B4B74A750EC8ECC3C4D8544A6A
SHA-512:	F7BD7BEC0F2E9F1A832B3AED4E184144FE8BD50745B656B6E59E8251FE80B98EC8DAB280986F49B3ADFCE9D57C0FD2ED8F856787E1211461B8486960C4EDA9B7
Malicious:	false
Preview:	w.FY...*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..238125000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-05-04 21:38:38.10][INFO][mr.Init] MR instance ID: 7292d652-dd55-4c6c-8231-2093a011d130\n","[2021-05-04 21:38:38.10][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-05-04 21:38:38.10][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-05-04 21:38:38.10][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-05-04 21:38:38.10][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-05-04 21:38:38.10][INFO][mr.CastProvider] Query enabled: true\n","[2021-05-04 21:38:38.10][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.150619344873859
Encrypted:	false
SSDEEP:	6:mTGWq2P923iKKdK8a2jMGIFUtpeaZmwPeATkwO923iKKdK8a2jMmLJ:7Wv45Kk8EFUtp9/PN5L5Kk8bJ
MD5:	5A3F81690615A9E49F5AA61EB8C200E4
SHA1:	13BB74FFB13D4A2F6AC526BF9DC392F6079FBF5E
SHA-256:	AEB6F86DFA786C239B338F6BB44D35C799011596C958E3AFF55D3F5EAB4B98B9
SHA-512:	A81C6616592BB55BE910700F33525F265D736ACB90330CFFF37239654CA0FFDF90C518194AD2CD7A359822CA3EF326973606A7629977FBC1A2C6221C0F633928
Malicious:	false
Preview:	2021/05/04-21:38:21.226 d80 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/05/04-21:38:21.233 d80 Recovering log #3.2021/05/04-21:38:21.244 d80 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.165904031722438
Encrypted:	false
SSDEEP:	6:mT7934q2P923iKKdKgXz4rRIFUtpe7ExJZmwPe7/n3DkwO923iKKdKgXz4q8LJ:MIv45KkgXiuFUtpT/Psz5L5KkgX2J
MD5:	B8BC015BD8D80BDDAC4B2E4C75F8A989
SHA1:	AB27AA5B14C4547F000C4C1F24D42A9FEFB57EB8
SHA-256:	4F6B639D2EC10D4F7B4957EDF79E5E9AF777825558C6F5FE81C17385B933DD78
SHA-512:	0338469D3F548A925F21C3EBBBA2E713506C2CD507E116BF1D53257FE21F23D68FB1ED27C0B772C5F03278CFDC9DC38E459EBEEB45BBCA1ADB76BEE4F25BAE74
Malicious:	false
Preview:	2021/05/04-21:38:21.513 1540 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/05/04-21:38:21.518 1540 Recovering log #3.2021/05/04-21:38:21.519 1540 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.9692823692710901
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUgZis6bCoTRsyl:wIElwQF8mpcSYN6tjqLF+ySnV1
MD5:	4BE4C838E4E4DE6D1E4C3E6F1EA4788D
SHA1:	B787A24CEF054EA1CBD1CA82A8B0309A74ADA085

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL	
SHA-256:	496F9536D1031CDA040B01E02FEE32AA274B6F4D3CBCEE20D8F3DB27D8AEA34C
SHA-512:	E8AD1EB139D7F4669AFAE2B5A7B5ECB753E126A6D97CB50BB0B0A226AE4416F4E29E20529940C3DD0D90941DA84486FA377A80BE3BF1A42DCEAD3CC22E67BC2B
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g...^.....j.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29252
Entropy (8bit):	0.6282849498115335
Encrypted:	false
SSDEEP:	48:84qkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUn4:84hIElwQF8mpcSs
MD5:	A98A2F8A8692A79315EB5AC11FC41DC3
SHA1:	3863DB43D33D81ED6161F8B16F8D6A0D100D4DA6
SHA-256:	37A5831CA65BE3D33827B8B616AD24DAC2E61C0F81162B0747AB205F63143E09
SHA-512:	B3D1819B50D318EBCDC701337A3C0828764C9D4B1E6EB2BF46F817B3C3B1F5CE817AF075FBCA25BC0AEDB92A8C6138F62CD0CEBE71CC49A1067642C57C75EEE
Malicious:	false
Preview:	.....f*&.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljljl:5ljljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946B
Malicious:	false
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.177189599495799
Encrypted:	false
SSDEEP:	6:mTpat+q2P923iKKdKrQMxIFUtpep5ZmwPeDKLVkwO923iKKdKrQMFLJ:kv45KkCFUtpy/PWKR5L5KktJ
MD5:	2832A25FA38A5BB2C3C3251CB962D954
SHA1:	D607EEE7956D8FEB894ED3E557B48F0E56C5594C
SHA-256:	8C61EB3CBD139BF02118B04FE76C000F76E2B521E1708201B2DFC5DC924F52BE
SHA-512:	4C4A5B9A76935CC04A2C9DCCA860CB9B4425ADB7B7AD65326D6533BB65C3BDA202AFB8E98989B602883B4AA943C431781976A60A31D4DA3BA77403F6648F8CA
Malicious:	false
Preview:	2021/05/04-21:38:21.434 16d8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/05/04-21:38:21.435 16d8 Recovering log #3.2021/05/04-21:38:21.436 16d8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Category:	dropped
Size (bytes):	350
Entropy (8bit):	5.136479081115454
Encrypted:	false
SSDEEP:	6:mT/Tq2P923iKKdK7Uh2ghZIFUtpe/V9ZmwPe/EkwO923iKKdK7Uh2gnLJ:2v45KkIhHh2FUtp69/PX5L5KkIhHLJ
MD5:	89C13CB4CCFC1B679EEFFB316932CCCC
SHA1:	B582AC2AA0A97E758AC35F754A1C7D8224DCC2DF
SHA-256:	BB8DB94FC0E50235F3AB3A00528CE09C5DA6BF0117F0A6B61AECA7D594652C52
SHA-512:	D0CB22A05C9FBFB54C9CAA3FB9B3E31BD553EA70091068529DD2D51ACF797D4F93DF1B0B97492A30B58A95AF443748C781BCC4C6584B3498CD12877205D91EC
Malicious:	false
Preview:	2021/05/04-21:38:21.142 1514 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/05/04-21:38:21.152 1514 Recovering log #3.2021/05/04-21:38:21.166 1514 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\10b9cad4-7dff-4d1c-b1c2-32538d1f314b.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):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","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):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Preview:	.'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.2583291615259755
Encrypted:	false
SSDEEP:	6:mTo4q2P923iKKdKusNpV/2jMGIFUtpe0JZmwPevNDkwO923iKKdKusNpV/2jMmLJ:+v45KkFFUtpj/P+5L5KkOJ
MD5:	760C4E1F5525DF28C40E22F8DDBF15E0
SHA1:	59047565B9B44E6A9445930BB63246BD53EDA87A
SHA-256:	7099A63BD9004F4BF947AD05CB7D88B20493535BF6AD5E5F32E850359773094A
SHA-512:	8B2A870E4A9CB6D1A0C840AA8E6A585D79693B6210C5FE4106A08D216922EC72D89997634621A49F3FD68B1D36A6EEEA2C5DE7A2ABD1B3C4CF584BEA75911FDE
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Preview:	2021/05/04-21:38:21.473 1540 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/05/04-21:38:21.477 1540 Recovering log #3.2021/05/04-21:38:21.478 1540 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	434
Entropy (8bit):	5.266933286641677
Encrypted:	false
SSDEEP:	6:mT7EO3+q2P923iKKdKusNpqz4rRIFUtpe7scZmwPe7scVkwO923iKKdKusNpqz4n:jv45KkmiuFUtpRc/PRc5L5Kkm2J
MD5:	C5E0BF6160FA6ABDD167B4C6E680B022
SHA1:	DE91275EDBB565E92C8DEBEEDEB40A2E89BAF079
SHA-256:	C764F55FA33454764B874B6BF675EB95C07DC745F5E9E5415524D3D7B8F76560
SHA-512:	051213EDD7BD7BA94102896E177F548ADE78318BBD23E0FE285EE7BD5A92B85CA22404C7321D8031513F8E5B4D68D68167379C8B71887DA50FA19C748FE34E8
Malicious:	false
Preview:	2021/05/04-21:38:21.518 16f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/05/04-21:38:21.521 16f8 Recovering log #3.2021/05/04-21:38:21.521 16f8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	420
Entropy (8bit):	5.302178064293459
Encrypted:	false
SSDEEP:	6:mTbR+q2P923iKKdKusNpZQMxIFUtpenZmwPe2tVkwO923iKKdKusNpZQMFLJ:Jv45KkMFUtpu/PZ5L5KkTJ
MD5:	6E3AC55FA230FDF0C9F4F81A89E6E8F4
SHA1:	33E7A15833D85C4A945B52DD0DCE6F46753EFCF3
SHA-256:	B896E5C3F0CB7AA8D801F9525D913E2E7F77B9D9F6B49184E16D6B2829BEA07C
SHA-512:	818A1CCAAAB78A40D2940CA3AC278A06C58D89051E828282AE69214ECF4694BD250654098DFCD3096EF7DA7243775DABD879DBC01DAAB8D8C7A49497671A39D
Malicious:	false
Preview:	2021/05/04-21:38:37.931 16f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/05/04-21:38:37.933 16f8 Recovering log #3.2021/05/04-21:38:37.934 16f8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	592
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E8E:8N
MD5:	B505641E5E90B7CF4BC869DD1B4BE451
SHA1:	0EC7B13DC043E054AB48B8F45FE49EF1209C01AA

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
SHA-256:	2755F85F14CF33404CEEBF053D0CB79DC3B98D643A51075737E6A5BE154FE1D9
SHA-512:	610AF095630C93B0586F4D9CA84FA75454C472C557D4FDBC0D5C1851F9AABF8653079A7ADE4659ABADDEDC2E02E58AD13C7244CD004B0AA5A462307F293F833
Malicious:	false
Preview:	.'..(.....'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.2318762995659505
Encrypted:	false
SSDEEP:	12:vyv45KkkGHArBFUtpBm/PsZR5L5KkkGHAryJ:vY45KkkGgPgLPZDL5KkkGga
MD5:	1CCCAEC205F9CEABD1647205DAF860C4
SHA1:	59A3DDF4AB0ABCD2C81794D44892C735CEF80C1F
SHA-256:	C617D691F34972FD8F66B21F1E21FE36D55E2F67494126F100BE835EBA09666D
SHA-512:	EF8DC72E627520C2F764E57C5096D7535D8DDC3AB706995DDF3BAB1E715DC09C791FFED70E9C7CDFF1839BC5D35947C5351B732E6DC3F4ABA43E3DA9844B071
Malicious:	false
Preview:	2021/05/04-21:38:35.749 15c4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/05/04-21:38:35.762 15c4 Recovering log #3.2021/05/04-21:38:35.777 15c4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	434
Entropy (8bit):	5.260569895712682
Encrypted:	false
SSDEEP:	12:2v45KkkGHArqiuFUtp//Ps35L5KkkGHArq2J:U45KkkGgCgqpL5KkkGg7
MD5:	7246DC3F5C29A8A7B72970A938BE5E76
SHA1:	FC4A1934415535E1EEA05AAD4E19BD2536B58EA3
SHA-256:	A5E256B846E7A5E38722E48A8B212C692EE8B9053A9CE07723CCC7DA23DB3846
SHA-512:	187462C5195563EA2AA04D9965D8338E65906D6D41D172D613B799FADEB068F1ECC49E01B3FC1373BD1FCD6C57DBB54CC3F82EA4CBC344C07D4FD5F09E0716
Malicious:	false
Preview:	2021/05/04-21:38:35.749 16f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/05/04-21:38:35.763 16f8 Recovering log #3.2021/05/04-21:38:35.777 16f8 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljl:5ljl
MD5:	E9C694B34731BF91073CF432768A9C44
SHA1:	861F5A99AD9EF017106CA6826EFE42413CDA1A0E
SHA-256:	01C766E2C0228436212045FA98D970A0AD1F1F73ABAA6A26E97C6639A4950D85
SHA-512:	2A359571C4326559459C881CBA4FF4FA9F312F6A7C2955B120B907430B700EA6FD42A48FBB3CC9F0CA2950D114DF036D1BB3B0618D137A36EBAAA17092FE5F0
Malicious:	false
Preview:	..&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	420

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Entropy (8bit):	5.214368138244304
Encrypted:	false
SSDEEP:	12:nv45KkkGHArAFUtpV5/PdcDT5L5KkkGHArfJ:v45KkkGgkgfLcL5KkkGgV
MD5:	9B543DA0E42C6BBF12B8BBE6034BAC74
SHA1:	70E3679F8CEC7E1E546A1CB5C3786B8BA6D5552E
SHA-256:	EA19A9B963E80CA50843ECC6C7C0A99F1EFF36495760B6B0DC4FA3F85536BE8A
SHA-512:	6B25BB0EF3848410CC38834B382259C92062397F4D0337321645B3C9D9770C5627EFB95D1A7FE06C67909AE5624CC0EF8FBC81C6CD24068A8DE9EBE5FEBBE23
Malicious:	false
Preview:	2021/05/04-21:38:51.384 16f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/05/04-21:38:51.390 16f8 Recovering log #3.2021/05/04-21:38:51.391 16f8 Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\ed8954d8-3f2b-4e1b-b29d-f26f5a04eaca.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):	325
Entropy (8bit):	4.976576189225149
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5OV/sDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdysBdLJlyH7E4f3K33y
MD5:	5886A009EB58EE06A16EFD6D1BA9A046
SHA1:	A867B5052F3FBB811693DF8CE3FDAA794F2F2E40
SHA-256:	9E3392126DE2D81D019E0AB3E17F20BADD0EC9FBD944BCB7C4DAF449D937D496
SHA-512:	D24F30A2E35F903AC10AACC4425C58BECB1C6BE2BA30A3C2B9D9D46CE04914AA71F55B3B16ED89081AD65A7090C77F5DC4A258B7B98D71E6A994D176536FB 27
Malicious:	false
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542597817103","port":443,"protocol_str":"quic"}],"isol ation":[],"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\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF21 24
Malicious:	false
Preview:	..F.....F.....

Static File Info

General

File type:	PDF document, version 1.4
Entropy (8bit):	7.8555115777710185
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	reflective_practice_template_nhs[1].pdf
File size:	77482
MD5:	bd93c6b39cf6fbfb5f2009a320f70ab2
SHA1:	bc2b60452dbe4994d0d1d8ab2a769b278a5cd58d
SHA256:	834c0a2229054d27ad6ce7ff422a332cd18694bd828c4a4 b3a4745b0086fe144
SHA512:	6ffd02d1814d431e47e35380d8486d83581c7ddbea3d8c4 1cc6f945cd9f729b268db10b8430a9522a68d88be8078c0 ef1887548645ed3d052ab8ba4ffeea5446

General

SSDEEP:	1536:aBIr7KJz2GYsWHJC6li6llkX7631diMy1qDmHg686/3OdoB4aKr2:aIqJRYDVdSlauaMyfHW6vOdoD
File Content Preview:	%PDF-1.4.1 0 obj.<<./Title (...R.e.f.l.e.c.t.i.v.e. .p.r.a.c.t.i.c.e. .t.e.m.p.l.a.t.e. .n.h.s)./Creator (...w.k.h.t.m.l.t.o.p.d.f. .0...1.2...5)./Producer (...Q.t. .4...8...7)./CreationDate (D:20201226070235+02'00').>>.endobj.3 0 obj.<<./Type /ExtGState.

File Icon

Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

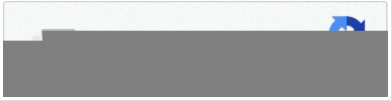
General

Header:	%PDF-1.4
Total Entropy:	7.855512
Total Bytes:	77482
Stream Entropy:	7.962804
Stream Bytes:	67016
Entropy outside Streams:	0.000000
Bytes outside Streams:	10466
Number of EOF found:	2
Bytes after EOF:	

Keywords Statistics

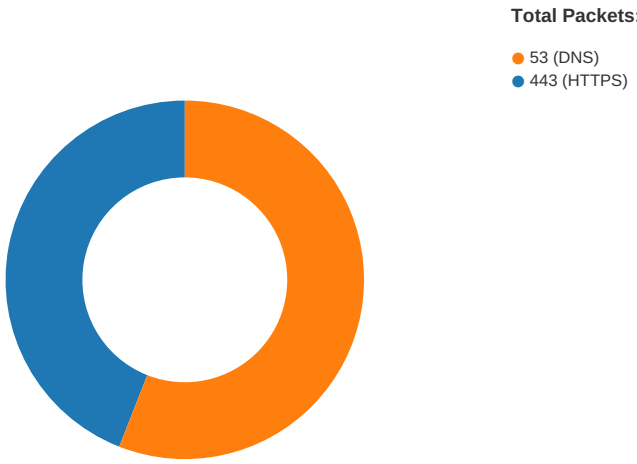
Name	Count
obj	59
endobj	59
stream	9
endstream	9
xref	2
trailer	2
startxref	2
/Page	3
/Encrypt	0
/ObjStm	0
/URI	36
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Image Streams

ID	DHASH	MD5	Preview
6	a384748d4c708482	daa2c2339df02c1e53080c829697ba54	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:38:26.499306917 CEST	49720	443	192.168.2.5	172.67.171.190
May 4, 2021 21:38:26.500466108 CEST	49721	443	192.168.2.5	172.67.171.190
May 4, 2021 21:38:26.546581984 CEST	443	49720	172.67.171.190	192.168.2.5
May 4, 2021 21:38:26.546673059 CEST	49720	443	192.168.2.5	172.67.171.190
May 4, 2021 21:38:26.548687935 CEST	49720	443	192.168.2.5	172.67.171.190
May 4, 2021 21:38:26.553060055 CEST	443	49721	172.67.171.190	192.168.2.5
May 4, 2021 21:38:26.553150892 CEST	49721	443	192.168.2.5	172.67.171.190
May 4, 2021 21:38:26.553466082 CEST	49721	443	192.168.2.5	172.67.171.190
May 4, 2021 21:38:26.598124981 CEST	443	49720	172.67.171.190	192.168.2.5
May 4, 2021 21:38:26.602190018 CEST	443	49720	172.67.171.190	192.168.2.5
May 4, 2021 21:38:26.602209091 CEST	443	49720	172.67.171.190	192.168.2.5
May 4, 2021 21:38:26.602276087 CEST	49720	443	192.168.2.5	172.67.171.190
May 4, 2021 21:38:26.607814074 CEST	443	49721	172.67.171.190	192.168.2.5
May 4, 2021 21:38:26.630072117 CEST	443	49721	172.67.171.190	192.168.2.5
May 4, 2021 21:38:26.630100012 CEST	443	49721	172.67.171.190	192.168.2.5
May 4, 2021 21:38:26.630148888 CEST	49721	443	192.168.2.5	172.67.171.190
May 4, 2021 21:38:26.896550894 CEST	49720	443	192.168.2.5	172.67.171.190
May 4, 2021 21:38:26.897952080 CEST	49721	443	192.168.2.5	172.67.171.190
May 4, 2021 21:38:26.898128986 CEST	49721	443	192.168.2.5	172.67.171.190
May 4, 2021 21:38:26.898354053 CEST	49720	443	192.168.2.5	172.67.171.190
May 4, 2021 21:38:26.899033070 CEST	49720	443	192.168.2.5	172.67.171.190
May 4, 2021 21:38:26.943882942 CEST	443	49720	172.67.171.190	192.168.2.5
May 4, 2021 21:38:26.944109917 CEST	443	49720	172.67.171.190	192.168.2.5
May 4, 2021 21:38:26.945487022 CEST	443	49720	172.67.171.190	192.168.2.5
May 4, 2021 21:38:26.945506096 CEST	443	49720	172.67.171.190	192.168.2.5
May 4, 2021 21:38:26.945570946 CEST	49720	443	192.168.2.5	172.67.171.190
May 4, 2021 21:38:26.950594902 CEST	443	49721	172.67.171.190	192.168.2.5
May 4, 2021 21:38:26.951157093 CEST	49720	443	192.168.2.5	172.67.171.190
May 4, 2021 21:38:26.951237917 CEST	443	49721	172.67.171.190	192.168.2.5
May 4, 2021 21:38:26.951297998 CEST	49721	443	192.168.2.5	172.67.171.190
May 4, 2021 21:38:26.988168955 CEST	443	49720	172.67.171.190	192.168.2.5
May 4, 2021 21:38:26.998384953 CEST	443	49720	172.67.171.190	192.168.2.5
May 4, 2021 21:38:27.365039110 CEST	443	49720	172.67.171.190	192.168.2.5
May 4, 2021 21:38:27.365052938 CEST	443	49720	172.67.171.190	192.168.2.5
May 4, 2021 21:38:27.365113974 CEST	49720	443	192.168.2.5	172.67.171.190
May 4, 2021 21:38:27.482130051 CEST	49731	443	192.168.2.5	35.190.80.1
May 4, 2021 21:38:27.526329994 CEST	443	49731	35.190.80.1	192.168.2.5
May 4, 2021 21:38:27.526408911 CEST	49731	443	192.168.2.5	35.190.80.1
May 4, 2021 21:38:27.526627064 CEST	49731	443	192.168.2.5	35.190.80.1
May 4, 2021 21:38:27.567907095 CEST	443	49731	35.190.80.1	192.168.2.5
May 4, 2021 21:38:27.569292068 CEST	443	49731	35.190.80.1	192.168.2.5
May 4, 2021 21:38:27.569314003 CEST	443	49731	35.190.80.1	192.168.2.5
May 4, 2021 21:38:27.569322109 CEST	443	49731	35.190.80.1	192.168.2.5
May 4, 2021 21:38:27.569498062 CEST	49731	443	192.168.2.5	35.190.80.1

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:38:27.581140041 CEST	49731	443	192.168.2.5	35.190.80.1
May 4, 2021 21:38:27.581270933 CEST	49731	443	192.168.2.5	35.190.80.1
May 4, 2021 21:38:27.581398964 CEST	49731	443	192.168.2.5	35.190.80.1
May 4, 2021 21:38:27.623140097 CEST	443	49731	35.190.80.1	192.168.2.5
May 4, 2021 21:38:27.623433113 CEST	443	49731	35.190.80.1	192.168.2.5
May 4, 2021 21:38:27.623440981 CEST	49731	443	192.168.2.5	35.190.80.1
May 4, 2021 21:38:27.663750887 CEST	49731	443	192.168.2.5	35.190.80.1
May 4, 2021 21:38:27.670895100 CEST	443	49731	35.190.80.1	192.168.2.5
May 4, 2021 21:38:27.728943110 CEST	443	49731	35.190.80.1	192.168.2.5
May 4, 2021 21:38:27.729798079 CEST	49731	443	192.168.2.5	35.190.80.1
May 4, 2021 21:38:27.729832888 CEST	49731	443	192.168.2.5	35.190.80.1
May 4, 2021 21:38:27.729990959 CEST	49731	443	192.168.2.5	35.190.80.1
May 4, 2021 21:38:27.730025053 CEST	49731	443	192.168.2.5	35.190.80.1
May 4, 2021 21:38:27.770852089 CEST	443	49731	35.190.80.1	192.168.2.5
May 4, 2021 21:38:27.772176027 CEST	443	49731	35.190.80.1	192.168.2.5
May 4, 2021 21:38:27.772202015 CEST	443	49731	35.190.80.1	192.168.2.5
May 4, 2021 21:38:27.772216082 CEST	443	49731	35.190.80.1	192.168.2.5
May 4, 2021 21:38:27.879060984 CEST	443	49731	35.190.80.1	192.168.2.5
May 4, 2021 21:38:27.879678965 CEST	49731	443	192.168.2.5	35.190.80.1
May 4, 2021 21:38:27.879744053 CEST	49731	443	192.168.2.5	35.190.80.1
May 4, 2021 21:38:27.922131062 CEST	443	49731	35.190.80.1	192.168.2.5
May 4, 2021 21:38:27.922154903 CEST	443	49731	35.190.80.1	192.168.2.5
May 4, 2021 21:38:35.825896978 CEST	49742	443	192.168.2.5	216.58.212.129
May 4, 2021 21:38:35.866630077 CEST	443	49742	216.58.212.129	192.168.2.5
May 4, 2021 21:38:35.866763115 CEST	49742	443	192.168.2.5	216.58.212.129
May 4, 2021 21:38:35.867098093 CEST	49742	443	192.168.2.5	216.58.212.129
May 4, 2021 21:38:35.907686949 CEST	443	49742	216.58.212.129	192.168.2.5
May 4, 2021 21:38:35.914891005 CEST	443	49742	216.58.212.129	192.168.2.5
May 4, 2021 21:38:35.914917946 CEST	443	49742	216.58.212.129	192.168.2.5
May 4, 2021 21:38:35.914930105 CEST	443	49742	216.58.212.129	192.168.2.5
May 4, 2021 21:38:35.914947033 CEST	443	49742	216.58.212.129	192.168.2.5
May 4, 2021 21:38:35.914963007 CEST	443	49742	216.58.212.129	192.168.2.5
May 4, 2021 21:38:35.914975882 CEST	443	49742	216.58.212.129	192.168.2.5
May 4, 2021 21:38:35.915021896 CEST	49742	443	192.168.2.5	216.58.212.129
May 4, 2021 21:38:35.915153980 CEST	49742	443	192.168.2.5	216.58.212.129
May 4, 2021 21:38:35.956248045 CEST	49742	443	192.168.2.5	216.58.212.129
May 4, 2021 21:38:35.956290007 CEST	49742	443	192.168.2.5	216.58.212.129
May 4, 2021 21:38:35.956568003 CEST	49742	443	192.168.2.5	216.58.212.129
May 4, 2021 21:38:35.998790026 CEST	443	49742	216.58.212.129	192.168.2.5
May 4, 2021 21:38:35.999592066 CEST	443	49742	216.58.212.129	192.168.2.5
May 4, 2021 21:38:35.999854088 CEST	49742	443	192.168.2.5	216.58.212.129
May 4, 2021 21:38:36.001430035 CEST	49742	443	192.168.2.5	216.58.212.129
May 4, 2021 21:38:36.001724958 CEST	443	49742	216.58.212.129	192.168.2.5
May 4, 2021 21:38:36.001769066 CEST	443	49742	216.58.212.129	192.168.2.5
May 4, 2021 21:38:36.002005100 CEST	49742	443	192.168.2.5	216.58.212.129
May 4, 2021 21:38:36.003222942 CEST	443	49742	216.58.212.129	192.168.2.5
May 4, 2021 21:38:36.003273964 CEST	443	49742	216.58.212.129	192.168.2.5
May 4, 2021 21:38:36.003361940 CEST	49742	443	192.168.2.5	216.58.212.129
May 4, 2021 21:38:36.006061077 CEST	443	49742	216.58.212.129	192.168.2.5
May 4, 2021 21:38:36.006102085 CEST	443	49742	216.58.212.129	192.168.2.5
May 4, 2021 21:38:36.006180048 CEST	49742	443	192.168.2.5	216.58.212.129
May 4, 2021 21:38:36.006253958 CEST	49742	443	192.168.2.5	216.58.212.129
May 4, 2021 21:38:36.008982897 CEST	443	49742	216.58.212.129	192.168.2.5
May 4, 2021 21:38:36.009037018 CEST	443	49742	216.58.212.129	192.168.2.5
May 4, 2021 21:38:36.009109020 CEST	49742	443	192.168.2.5	216.58.212.129
May 4, 2021 21:38:36.009233952 CEST	49742	443	192.168.2.5	216.58.212.129

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:37:08.559087038 CEST	54302	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:08.610784054 CEST	53	54302	8.8.8.8	192.168.2.5
May 4, 2021 21:37:09.684544086 CEST	53784	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:09.736143112 CEST	53	53784	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:37:10.733546972 CEST	65307	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:10.782202959 CEST	53	65307	8.8.8.8	192.168.2.5
May 4, 2021 21:37:11.574794054 CEST	64344	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:11.604474068 CEST	62060	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:11.623424053 CEST	53	64344	8.8.8.8	192.168.2.5
May 4, 2021 21:37:11.661849976 CEST	53	62060	8.8.8.8	192.168.2.5
May 4, 2021 21:37:11.970403910 CEST	61805	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:12.023178101 CEST	53	61805	8.8.8.8	192.168.2.5
May 4, 2021 21:37:12.251667976 CEST	54795	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:12.300272942 CEST	53	54795	8.8.8.8	192.168.2.5
May 4, 2021 21:37:12.804617882 CEST	49557	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:12.853354931 CEST	53	49557	8.8.8.8	192.168.2.5
May 4, 2021 21:37:14.100409031 CEST	61733	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:14.151990891 CEST	53	61733	8.8.8.8	192.168.2.5
May 4, 2021 21:37:14.999650002 CEST	65447	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:15.061435938 CEST	53	65447	8.8.8.8	192.168.2.5
May 4, 2021 21:37:15.845446110 CEST	52441	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:15.910669088 CEST	53	52441	8.8.8.8	192.168.2.5
May 4, 2021 21:37:16.822905064 CEST	62176	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:16.874618053 CEST	53	62176	8.8.8.8	192.168.2.5
May 4, 2021 21:37:18.192969084 CEST	59596	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:18.241823912 CEST	53	59596	8.8.8.8	192.168.2.5
May 4, 2021 21:37:19.781933069 CEST	65296	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:19.833367109 CEST	53	65296	8.8.8.8	192.168.2.5
May 4, 2021 21:37:27.594858885 CEST	63183	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:27.655883074 CEST	53	63183	8.8.8.8	192.168.2.5
May 4, 2021 21:37:33.514880896 CEST	56969	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:33.525307894 CEST	60151	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:33.578533888 CEST	53	56969	8.8.8.8	192.168.2.5
May 4, 2021 21:37:33.584152937 CEST	53	60151	8.8.8.8	192.168.2.5
May 4, 2021 21:37:34.509531975 CEST	56969	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:34.556298971 CEST	60151	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:34.572967052 CEST	53	56969	8.8.8.8	192.168.2.5
May 4, 2021 21:37:34.614694118 CEST	53	60151	8.8.8.8	192.168.2.5
May 4, 2021 21:37:34.791640997 CEST	55161	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:34.840599060 CEST	53	55161	8.8.8.8	192.168.2.5
May 4, 2021 21:37:35.525068998 CEST	56969	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:35.525130987 CEST	60151	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:35.577987909 CEST	53	56969	8.8.8.8	192.168.2.5
May 4, 2021 21:37:35.583508968 CEST	53	60151	8.8.8.8	192.168.2.5
May 4, 2021 21:37:37.574147940 CEST	60151	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:37.574263096 CEST	56969	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:37.631937981 CEST	53	60151	8.8.8.8	192.168.2.5
May 4, 2021 21:37:37.634584904 CEST	53	56969	8.8.8.8	192.168.2.5
May 4, 2021 21:37:41.585550070 CEST	56969	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:41.585697889 CEST	60151	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:41.645651102 CEST	53	60151	8.8.8.8	192.168.2.5
May 4, 2021 21:37:41.645669937 CEST	53	56969	8.8.8.8	192.168.2.5
May 4, 2021 21:37:47.127182007 CEST	54757	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:47.189827919 CEST	53	54757	8.8.8.8	192.168.2.5
May 4, 2021 21:37:53.462018967 CEST	49992	53	192.168.2.5	8.8.8.8
May 4, 2021 21:37:53.510936975 CEST	53	49992	8.8.8.8	192.168.2.5
May 4, 2021 21:38:01.786271095 CEST	60075	53	192.168.2.5	8.8.8.8
May 4, 2021 21:38:01.852391005 CEST	53	60075	8.8.8.8	192.168.2.5
May 4, 2021 21:38:03.014508963 CEST	55016	53	192.168.2.5	8.8.8.8
May 4, 2021 21:38:03.155760050 CEST	53	55016	8.8.8.8	192.168.2.5
May 4, 2021 21:38:10.064364910 CEST	64345	53	192.168.2.5	8.8.8.8
May 4, 2021 21:38:10.127238035 CEST	53	64345	8.8.8.8	192.168.2.5
May 4, 2021 21:38:26.434644938 CEST	50394	53	192.168.2.5	8.8.8.8
May 4, 2021 21:38:26.443581104 CEST	58530	53	192.168.2.5	8.8.8.8
May 4, 2021 21:38:26.444751024 CEST	53813	53	192.168.2.5	8.8.8.8
May 4, 2021 21:38:26.444777966 CEST	63732	53	192.168.2.5	8.8.8.8
May 4, 2021 21:38:26.445281982 CEST	57344	53	192.168.2.5	8.8.8.8
May 4, 2021 21:38:26.491827011 CEST	53	50394	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:38:26.501107931 CEST	53	58530	8.8.8.8	192.168.2.5
May 4, 2021 21:38:26.501903057 CEST	53	53813	8.8.8.8	192.168.2.5
May 4, 2021 21:38:26.510008097 CEST	53	57344	8.8.8.8	192.168.2.5
May 4, 2021 21:38:26.522717953 CEST	53	63732	8.8.8.8	192.168.2.5
May 4, 2021 21:38:27.103092909 CEST	54450	53	192.168.2.5	8.8.8.8
May 4, 2021 21:38:27.127974987 CEST	59261	53	192.168.2.5	8.8.8.8
May 4, 2021 21:38:27.151566029 CEST	53	54450	8.8.8.8	192.168.2.5
May 4, 2021 21:38:27.187886953 CEST	53	59261	8.8.8.8	192.168.2.5
May 4, 2021 21:38:27.379429102 CEST	57151	53	192.168.2.5	8.8.8.8
May 4, 2021 21:38:27.437839031 CEST	53	57151	8.8.8.8	192.168.2.5
May 4, 2021 21:38:31.917692900 CEST	65086	53	192.168.2.5	8.8.8.8
May 4, 2021 21:38:31.969430923 CEST	53	65086	8.8.8.8	192.168.2.5
May 4, 2021 21:38:35.767182112 CEST	61004	53	192.168.2.5	8.8.8.8
May 4, 2021 21:38:35.823765039 CEST	53	61004	8.8.8.8	192.168.2.5
May 4, 2021 21:38:36.484782934 CEST	56895	53	192.168.2.5	8.8.8.8
May 4, 2021 21:38:36.541830063 CEST	53	56895	8.8.8.8	192.168.2.5
May 4, 2021 21:38:38.394484997 CEST	62372	53	192.168.2.5	8.8.8.8
May 4, 2021 21:38:38.453613997 CEST	53	62372	8.8.8.8	192.168.2.5
May 4, 2021 21:38:45.240171909 CEST	61515	53	192.168.2.5	8.8.8.8
May 4, 2021 21:38:45.300102949 CEST	53	61515	8.8.8.8	192.168.2.5
May 4, 2021 21:39:04.474723101 CEST	56675	53	192.168.2.5	8.8.8.8
May 4, 2021 21:39:04.532016039 CEST	53	56675	8.8.8.8	192.168.2.5
May 4, 2021 21:39:05.087537050 CEST	57172	53	192.168.2.5	8.8.8.8
May 4, 2021 21:39:05.145929098 CEST	53	57172	8.8.8.8	192.168.2.5
May 4, 2021 21:39:22.280915022 CEST	55267	53	192.168.2.5	8.8.8.8
May 4, 2021 21:39:22.341516018 CEST	53	55267	8.8.8.8	192.168.2.5
May 4, 2021 21:39:22.713802099 CEST	64362	53	192.168.2.5	8.8.8.8
May 4, 2021 21:39:22.776351929 CEST	53	64362	8.8.8.8	192.168.2.5
May 4, 2021 21:39:22.915477991 CEST	54766	53	192.168.2.5	8.8.8.8
May 4, 2021 21:39:22.972810030 CEST	53	54766	8.8.8.8	192.168.2.5
May 4, 2021 21:39:23.426322937 CEST	61446	53	192.168.2.5	8.8.8.8
May 4, 2021 21:39:23.483385086 CEST	53	61446	8.8.8.8	192.168.2.5
May 4, 2021 21:39:49.120502949 CEST	57515	53	192.168.2.5	8.8.8.8
May 4, 2021 21:39:49.271924019 CEST	53	57515	8.8.8.8	192.168.2.5
May 4, 2021 21:39:50.290090084 CEST	58199	53	192.168.2.5	8.8.8.8
May 4, 2021 21:39:50.427409887 CEST	53	58199	8.8.8.8	192.168.2.5
May 4, 2021 21:39:51.934153080 CEST	65221	53	192.168.2.5	8.8.8.8
May 4, 2021 21:39:51.996319056 CEST	53	65221	8.8.8.8	192.168.2.5
May 4, 2021 21:39:52.731506109 CEST	61573	53	192.168.2.5	8.8.8.8
May 4, 2021 21:39:52.792057037 CEST	53	61573	8.8.8.8	192.168.2.5
May 4, 2021 21:39:53.431478977 CEST	56562	53	192.168.2.5	8.8.8.8
May 4, 2021 21:39:53.495619059 CEST	53	56562	8.8.8.8	192.168.2.5
May 4, 2021 21:39:54.963440895 CEST	53591	53	192.168.2.5	8.8.8.8
May 4, 2021 21:39:55.022805929 CEST	53	53591	8.8.8.8	192.168.2.5
May 4, 2021 21:39:55.978914022 CEST	59688	53	192.168.2.5	8.8.8.8
May 4, 2021 21:39:56.040400982 CEST	53	59688	8.8.8.8	192.168.2.5
May 4, 2021 21:39:57.449687004 CEST	56032	53	192.168.2.5	8.8.8.8
May 4, 2021 21:39:57.508286953 CEST	53	56032	8.8.8.8	192.168.2.5
May 4, 2021 21:39:59.670135975 CEST	61150	53	192.168.2.5	8.8.8.8
May 4, 2021 21:39:59.729918957 CEST	53	61150	8.8.8.8	192.168.2.5
May 4, 2021 21:40:00.479609966 CEST	63458	53	192.168.2.5	8.8.8.8
May 4, 2021 21:40:00.537863970 CEST	53	63458	8.8.8.8	192.168.2.5
May 4, 2021 21:40:28.229605913 CEST	50422	53	192.168.2.5	8.8.8.8
May 4, 2021 21:40:28.288954973 CEST	53	50422	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 21:38:10.064364910 CEST	192.168.2.5	8.8.8.8	0xecd	Standard query (0)	traffking.ru	A (IP address)	IN (0x0001)
May 4, 2021 21:38:26.434644938 CEST	192.168.2.5	8.8.8.8	0x110	Standard query (0)	traffking.ru	A (IP address)	IN (0x0001)
May 4, 2021 21:38:27.379429102 CEST	192.168.2.5	8.8.8.8	0x6733	Standard query (0)	a.nel.cloudflare.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 21:38:35.767182112 CEST	192.168.2.5	8.8.8.8	0xf3d7	Standard query (0)	clients2.google usercontent.com	A (IP address)	IN (0x0001)

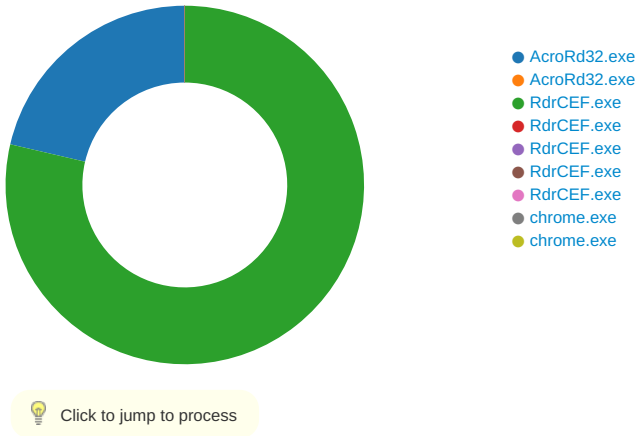
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:38:10.127238035 CEST	8.8.8.8	192.168.2.5	0xecd	No error (0)	traffking.ru		172.67.171.190	A (IP address)	IN (0x0001)
May 4, 2021 21:38:10.127238035 CEST	8.8.8.8	192.168.2.5	0xecd	No error (0)	traffking.ru		104.21.71.213	A (IP address)	IN (0x0001)
May 4, 2021 21:38:26.491827011 CEST	8.8.8.8	192.168.2.5	0x110	No error (0)	traffking.ru		172.67.171.190	A (IP address)	IN (0x0001)
May 4, 2021 21:38:26.491827011 CEST	8.8.8.8	192.168.2.5	0x110	No error (0)	traffking.ru		104.21.71.213	A (IP address)	IN (0x0001)
May 4, 2021 21:38:27.437839031 CEST	8.8.8.8	192.168.2.5	0x6733	No error (0)	a.nel.cloudflare.com		35.190.80.1	A (IP address)	IN (0x0001)
May 4, 2021 21:38:35.823765039 CEST	8.8.8.8	192.168.2.5	0xf3d7	No error (0)	clients2.google usercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:38:35.823765039 CEST	8.8.8.8	192.168.2.5	0xf3d7	No error (0)	googlehosted.l.googleusercontent.com		216.58.212.129	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: 6180 Parent PID: 5692

General

Start time:	21:37:14
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\reflective_practice_template_nhs[1].pdf'
Imagebase:	0x990000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx	read data or list directory | read attributes | write attributes | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	9C65C3	CreateDirectoryExW
C:\Users\user\AppData\Local\Temp\acrocef_low	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	9EAE05	CreateDirectoryW
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident	success or wait	1	9DEA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210505043724Z-239.bmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	9DEA85	NtCreateFile
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A583C8	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A583C8	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A583C8	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A583C8	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A583C8	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	A583C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rmboiu5_8pyshb_4u4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	9DEA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	3	9DEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R5ybqq7_8pyshc_4u4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	9DEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1498v9c_8pyshd_4u4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	9DEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Rsa3jyb_8pyshe_4u4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	9DEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1lqj7sf_8pyshf_4u4.tmp	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	9DEA85	NtCreateFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\System\Acrobatbrokerserverdispatchercpp789	success or wait	1	9DCF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	9DD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	9DD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0 \cTab0\cPathInfo	success or wait	1	9DD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\NoTimeOut	success or wait	1	9DD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	99EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	99EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	99EA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\TrustManager	success or wait	1	9DD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\TrustManager\cDefaultLaunchURLPerms	success or wait	1	9DD41D	NtCreateKey

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	aFS	unicode	DOS	success or wait	1	9EDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/reflecti ve_practice_template_nhs[1].pdf	success or wait	1	9EDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	reflective_practice_template_nhs[1].pdf	success or wait	1	9EDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	9EDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	9EDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDI	binary	2F 43 2F 55 73 65 72 73 2F 61 6C 66 6F 6E 73 2F 44 65 73 6B 74 6F 70 2F 72 65 66 6C 65 63 74 69 76 65 5F 70 72 61 63 74 69 63 65 5F 74 65 6D 70 6C 61 74 65 5F 6E 68 73 5B 31 5D 2E 70 64 66 00	success or wait	1	9EDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 31 30 35 30 34 32 31 33 37 32 33 2D 30 37 27 30 30 27 00	success or wait	1	9EDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	77482	success or wait	1	9EDF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	3	success or wait	1	9EDF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	9EDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tDIText	unicode	http://www.adobe.com/go/homeac rordrunified18_2018	success or wait	1	9EDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	9EDF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	9EDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDI	binary	68 74 74 70 3A 2F 2F 77 77 77 2E 61 64 6F 62 65 2E 63 6F 6D 2F 67 6F 2F 68 6F 6D 65 61 63 72 6F 72 64 72 75 6E 69 66 69 65 64 31 38 5F 32 30 31 38 00	success or wait	1	9EDF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sDate	binary	44 3A 32 30 31 39 30 36 32 37 31 31 33 35 32 30 2D 30 37 27 30 30 27 00	success or wait	1	9EDF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 6268 Parent PID: 6180

General

Start time:	21:37:15
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe

Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\reflective_practice_template_nhs[1].pdf'
Imagebase:	0x990000
File size:	2571312 bytes
MD5 hash:	B969CF0C7B2C443A99034881E8C8740A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: RdrCEF.exe PID: 6488 Parent PID: 6180

General

Start time:	21:37:23
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043
Imagebase:	0x9b0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	3	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	3	AA59E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	10	AB83E5	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	40	AB8447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	161	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	3	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	5	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	3	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	17	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	3	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	4	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	success or wait	8	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	1088	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	29	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	5	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	4	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	success or wait	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	success or wait	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	success or wait	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	success or wait	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\selector.js	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	success or wait	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	success or wait	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	end of file	2	AA59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	success or wait	12	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	success or wait	12	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	success or wait	28	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	success or wait	30	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	success or wait	43	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	27	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	30	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	success or wait	10	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	10	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	10	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	success or wait	8	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	144	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	120	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	success or wait	134	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	24	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	success or wait	97	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	16	AA59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	3	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main-selector.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main-selector.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main-selector.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	success or wait	3	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\css\main.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\css\main.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	4	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	success or wait	84	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	success or wait	4	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\plugin.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main-selector.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main-selector.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\css\main-selector.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main-selector.css	unknown	4096	end of file	1	AA59E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	success or wait	8	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\css\main.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\css\main.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	success or wait	163	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\css\main.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\selector.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\selector.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\css\main-selector.css	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\selector.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	success or wait	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\selector.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	success or wait	75	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\scan-files\js\plugin.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	success or wait	6	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-computer\js\plugin.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	success or wait	16	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\activity-badge\js\plugin.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	success or wait	5	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\js\plugin.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	success or wait	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\search-summary\js\selector.js	unknown	4096	end of file	1	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	success or wait	2	AA59E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-recent-files\js\selector.js	unknown	4096	end of file	1	AA59E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	AB83E5	ReadFile

Analysis Process: RdrCEF.exe PID: 6784 Parent PID: 6488

General

Start time:	21:37:26
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1588,520769569228620 8694,13668873235774985554,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=4477307787754487931 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=4477307787754487931 --renderer-client-id=2 --mojo-platform-channel-handle=1716 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x9b0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 6832 Parent PID: 6488

General

Start time:	21:37:27
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1588,5207695692286208694,13668873235774985554,131072 --disable-features=VizDisplayCompositor --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --lang=en-US --gpu-preferences=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=5528301929327232026 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0x9b0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 6912 Parent PID: 6488

General

Start time:	21:37:32
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1588,520769569228620 8694,13668873235774985554,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=9756364306558423637 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=9756364306558423637 --renderer-client-id=4 --mojo-platform-channel-handle=1824 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x7ff797770000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RdrCEF.exe PID: 5984 Parent PID: 6488

General

Start time:	21:37:39
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=renderer --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --touch-events=enabled --field-trial-handle=1588,520769569228620 8694,13668873235774985554,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=7523555841818072242 --lang=en-US --disable-pack-loading --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --log-severity=disable --product-version='ReaderServices/19.12.20035 Chrome/80.0.0.0' --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --service-request-channel-token=7523555841818072242 --renderer-client-id=5 --mojo-platform-channel-handle=2224 --allow-no-sandbox-job /prefetch:1
Imagebase:	0x9b0000
File size:	9475120 bytes
MD5 hash:	9AEBA3BACD721484391D15478A4080C7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: 5228 Parent PID: 6180

General

Start time:	21:38:19
Start date:	04/05/2021

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://traffking.ru/square?utm_term=reflective+practice+template+nhs'
Imagebase:	0x7ff75a8c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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

Analysis Process: chrome.exe PID: 5564 Parent PID: 5228

General

Start time:	21:38:21
Start date:	04/05/2021
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=1560,17001144406219017590,14380291932932443674,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1824 /prefetch:8
Imagebase:	0x7ff75a8c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly

Code Analysis