



ID: 356294
Sample Name: JTI NETWORK - Proposal & Quote.pdf
Cookbook: defaultwindowspdfcookbook.jbs
Time: 21:19:44
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report JTI NETWORK - Proposal & Quote.pdf 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 5
Yara Overview 5
Dropped Files 5
Sigma Overview 5
Signature Overview 5
AV Detection: 6
Phishing: 6
Compliance: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 13
Public 14
Private 14
General Information 14
Simulations 17
Behavior and APIs 17
Joe Sandbox View / Context 17
IPs 17
Domains 18
ASN 19
JA3 Fingerprints 20
Dropped Files 21
Created / dropped Files 21
Static File Info 51
General 51
File Icon 52
Static PDF Info 52
General 52
Keywords Statistics 52
Network Behavior 52
Network Port Distribution 52
TCP Packets 53
UDP Packets 54
DNS Queries 57
DNS Answers 57
HTTPS Packets 58

Code Manipulations 59
Statistics 59
Behavior 59
System Behavior 59
Analysis Process: AcroRd32.exe PID: 404 Parent PID: 5684 59
General 59
File Activities 60
File Created 60
File Moved 62
Registry Activities 62
Key Created 62
Key Value Created 62
Analysis Process: AcroRd32.exe PID: 5820 Parent PID: 404 63
General 63
File Activities 63
Registry Activities 63
Analysis Process: RdrCEF.exe PID: 6160 Parent PID: 404 63
General 63
File Activities 64
File Read 64
Analysis Process: RdrCEF.exe PID: 6324 Parent PID: 6160 68
General 68
File Activities 68
Analysis Process: RdrCEF.exe PID: 6352 Parent PID: 6160 69
General 69
File Activities 69
Analysis Process: RdrCEF.exe PID: 6400 Parent PID: 6160 69
General 69
File Activities 69
Analysis Process: RdrCEF.exe PID: 6528 Parent PID: 6160 69
General 70
File Activities 70
Analysis Process: RdrCEF.exe PID: 6812 Parent PID: 6160 70
General 70
File Activities 70
Analysis Process: iexplore.exe PID: 5480 Parent PID: 404 70
General 70
File Activities 71
Registry Activities 71
Analysis Process: iexplore.exe PID: 3864 Parent PID: 5480 71
General 71
File Activities 71
Disassembly 71
Code Analysis 72

Copyright null 2021

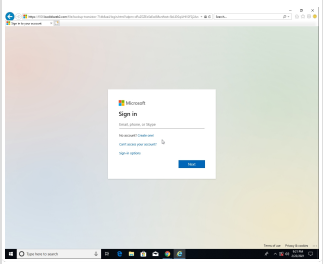
Analysis Report JTI NETWORK - Proposal & Quote.pdf

Overview

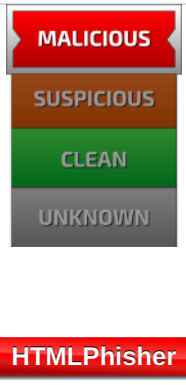
General Information

Sample Name:	JTI NETWORK - Proposal & Quote.pdf
Analysis ID:	356294
MD5:	29ea2103459376..
SHA1:	e9236798b8010c..
SHA256:	f6724cc9d5c2d6e..

Most interesting Screenshot:



Detection



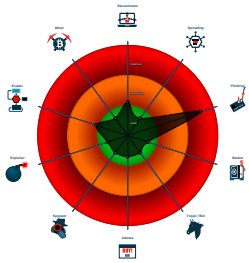
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- Machine Learning detection for samp…
- Phishing site detected (based on log…
- Contains functionality to access load…
- Found iframes
- HTML body contains low number of …
- HTML title does not match URL
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Submit button contains javascript call

Classification



Startup

- **System is w10x64**
- AcroRd32.exe (PID: 404 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' 'C:\Users\user\Desktop\JTI NETWORK - Proposal & Quote.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - AcroRd32.exe (PID: 5820 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe' --type=renderer /prefetch:1 'C:\Users\user\Desktop\JTI NETWORK - Proposal & Quote.pdf' MD5: B969CF0C7B2C443A99034881E8C8740A)
  - RdrCEF.exe (PID: 6160 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --backgroundcolor=16514043 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6324 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=1704,7748200756205629781,9837122587400820282,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=208034491646861541 --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=208034491646861541 --renderer-client-id=2 --mojo-platform-channel-handle=1712 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6352 cmdline: 'C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe' --type=gpu-process --field-trial-handle=1704,7748200756205629781,9837122587400820282,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=15924002696545913488 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6400 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=1704,7748200756205629781,9837122587400820282,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=965315283223708852 --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=965315283223708852 --renderer-client-id=4 --mojo-platform-channel-handle=1856 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6528 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=1704,7748200756205629781,9837122587400820282,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=9191971644911134211 --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=9191971644911134211 --renderer-client-id=5 --mojo-platform-channel-handle=1872 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
    - RdrCEF.exe (PID: 6812 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=1704,7748200756205629781,9837122587400820282,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6515428939137668262 --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=6515428939137668262 --renderer-client-id=6 --mojo-platform-channel-handle=2148 --allow-no-sandbox-job /prefetch:1 MD5: 9AEBA3BACD721484391D15478A4080C7)
  - iexplore.exe (PID: 5480 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' https://f000.backblazeb2.com/file/backup-transistor-71db8aa4/index.html MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 3864 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5480 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Copyright null 2021

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\index[1].htm	SUSP_Base64_Encoded_Hex_Encoded_Code	Detects hex encoded code that has been base64 encoded	Florian Roth	• 0x675:$x1: 78 34 4E 6A 56 63 65 44 63 30 58 48 67 • 0x685:$x1: 78 34 4E 7A 4A 63 65 44 5A 6C 58 48 67 • 0x6b5:$x1: 78 34 4E 6A 68 63 65 44 59 35 58 48 67 • 0x6e9:$x1: 78 34 4E 7A 4A 63 65 44 59 31 58 48 67 • 0x6f9:$x1: 78 34 4E 7A 52 63 65 44 59 31 58 48 67 • 0x709:$x1: 78 34 4E 6D 4E 63 65 44 59 31 58 48 67 • 0x719:$x1: 78 34 4E 6A 56 63 65 44 5A 6C 58 48 67 • 0x72d:$x1: 78 34 4E 6A 4E 63 65 44 59 78 58 48 67 • 0x751:$x1: 78 34 4E 6D 5A 63 65 44 5A 6B 58 48 67 • 0x761:$x1: 78 34 4E 6A 68 63 65 44 59 78 58 48 67 • 0x771:$x1: 78 34 4E 44 4E 63 65 44 5A 6D 58 48 67 • 0x795:$x1: 78 34 4E 7A 52 63 65 44 55 77 58 48 67 • 0x7a5:$x1: 78 34 4E 7A 4A 63 65 44 59 31 58 48 67 • 0x7c9:$x1: 78 34 4E 6A 6C 63 65 44 59 79 58 48 67 • 0x7d9:$x1: 78 34 4E 44 52 63 65 44 59 31 58 48 67 • 0x7e9:$x1: 78 34 4E 6D 4E 63 65 44 59 78 58 48 67 • 0x80d:$x1: 78 34 4E 6D 56 63 65 44 59 31 58 48 67 • 0x81d:$x1: 78 34 4E 44 68 63 65 44 55 30 58 48 67 • 0x841:$x1: 78 34 4E 6A 6C 63 65 44 59 7A 58 48 67 • 0x855:$x1: 78 34 4E 6A 6C 63 65 44 5A 6C 58 48 67 • 0x865:$x1: 78 34 4E 6A 46 63 65 44 5A 6A 58 48 67
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\login[1].htm	SUSP_Base64_Encoded_Hex_Encoded_Code	Detects hex encoded code that has been base64 encoded	Florian Roth	• 0x331d:$x1: 78 34 4E 7A 5A 63 65 44 59 78 58 48 67 • 0x332d:$x1: 78 34 4E 6A 6C 63 65 44 59 30 58 48 67 • 0x333d:$x1: 78 34 4E 6A 4E 63 65 44 5A 6D 58 48 67 • 0x334d:$x1: 78 34 4E 7A 42 63 65 44 63 79 58 48 67 • 0x335d:$x1: 78 34 4E 7A 4E 63 65 44 63 7A 58 48 67 • 0x336d:$x1: 78 34 4E 6D 5A 63 65 44 5A 6C 58 48 67 • 0x337d:$x1: 78 34 4E 7A 52 63 65 44 63 35 58 48 67 • 0x33a1:$x1: 78 34 4E 6A 5A 63 65 44 59 32 58 48 67 • 0x33c5:$x1: 78 34 4E 7A 5A 63 65 44 59 78 58 48 67 • 0x33d5:$x1: 78 34 4E 6A 6C 63 65 44 59 30 58 48 67 • 0x33e5:$x1: 78 34 4E 7A 56 63 65 44 5A 6C 58 48 67 • 0x33f5:$x1: 78 34 4E 6D 5A 63 65 44 5A 6B 58 48 67 • 0x3405:$x1: 78 34 4E 7A 4A 63 65 44 59 31 58 48 67 • 0x3415:$x1: 78 34 4E 7A 4E 63 65 44 59 31 58 48 67 • 0x3435:$x1: 78 34 4E 6D 5A 63 65 44 59 7A 58 48 67 • 0x3455:$x1: 78 34 4E 6A 46 63 65 44 59 30 58 48 67 • 0x3465:$x1: 78 34 4E 7A 4A 63 65 44 4E 68 58 48 67 • 0x3475:$x1: 78 34 4E 47 56 63 65 44 52 6A 58 48 67 • 0x3499:$x1: 78 34 4E 6A 4A 63 65 44 59 78 58 48 67 • 0x34a9:$x1: 78 34 4E 7A 4A 63 65 44 59 78 58 48 67 • 0x34bd:$x1: 78 34 4E 7A 52 63 65 44 59 31 58 48 67

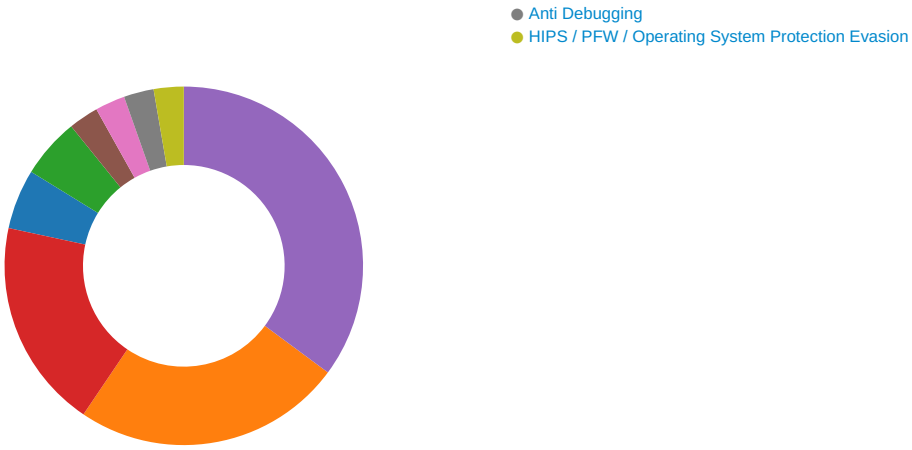
Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Phishing
- Compliance
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion

Copyright null 2021



AV Detection:



Antivirus detection for URL or domain

Machine Learning detection for sample

Phishing:



Phishing site detected (based on favicon image match)

Yara detected HtmlPhish_10

Phishing site detected (based on logo template match)

Compliance:



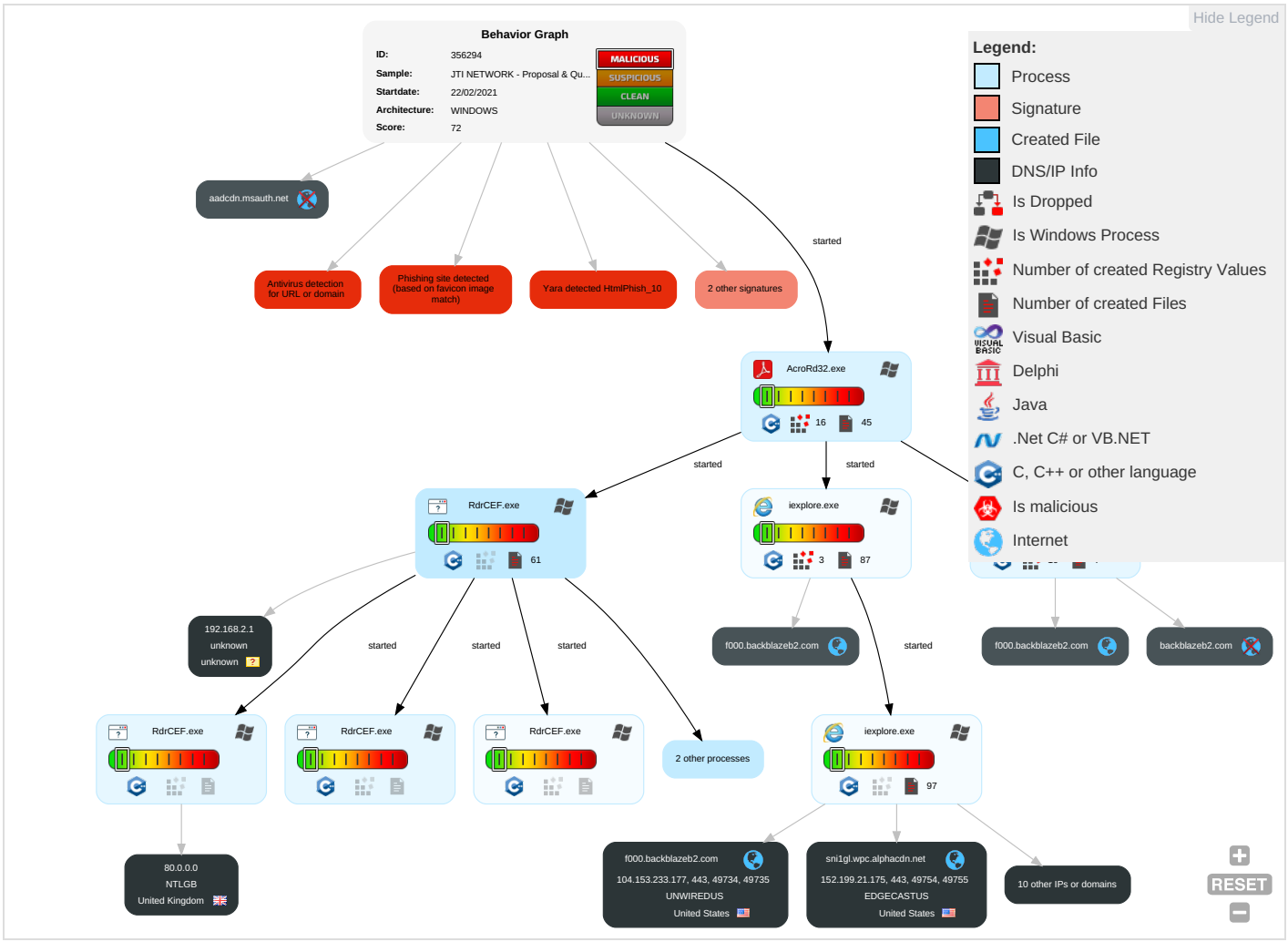
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

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	Im
Spearphishing Link 1	Scripting 1	Path Interception	Process Injection 2	Masquerading 1	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 Sy Pa
Drive-by Compromise 1	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 Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	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

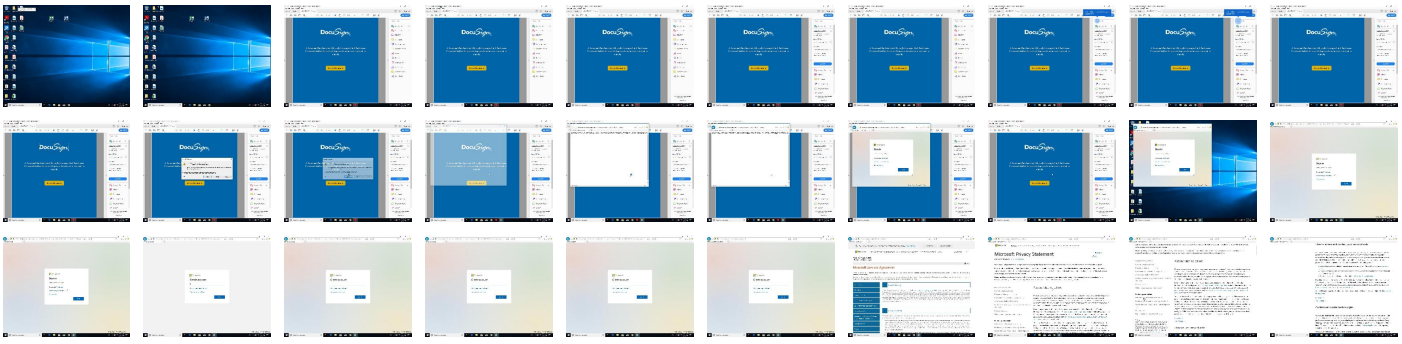
Behavior Graph

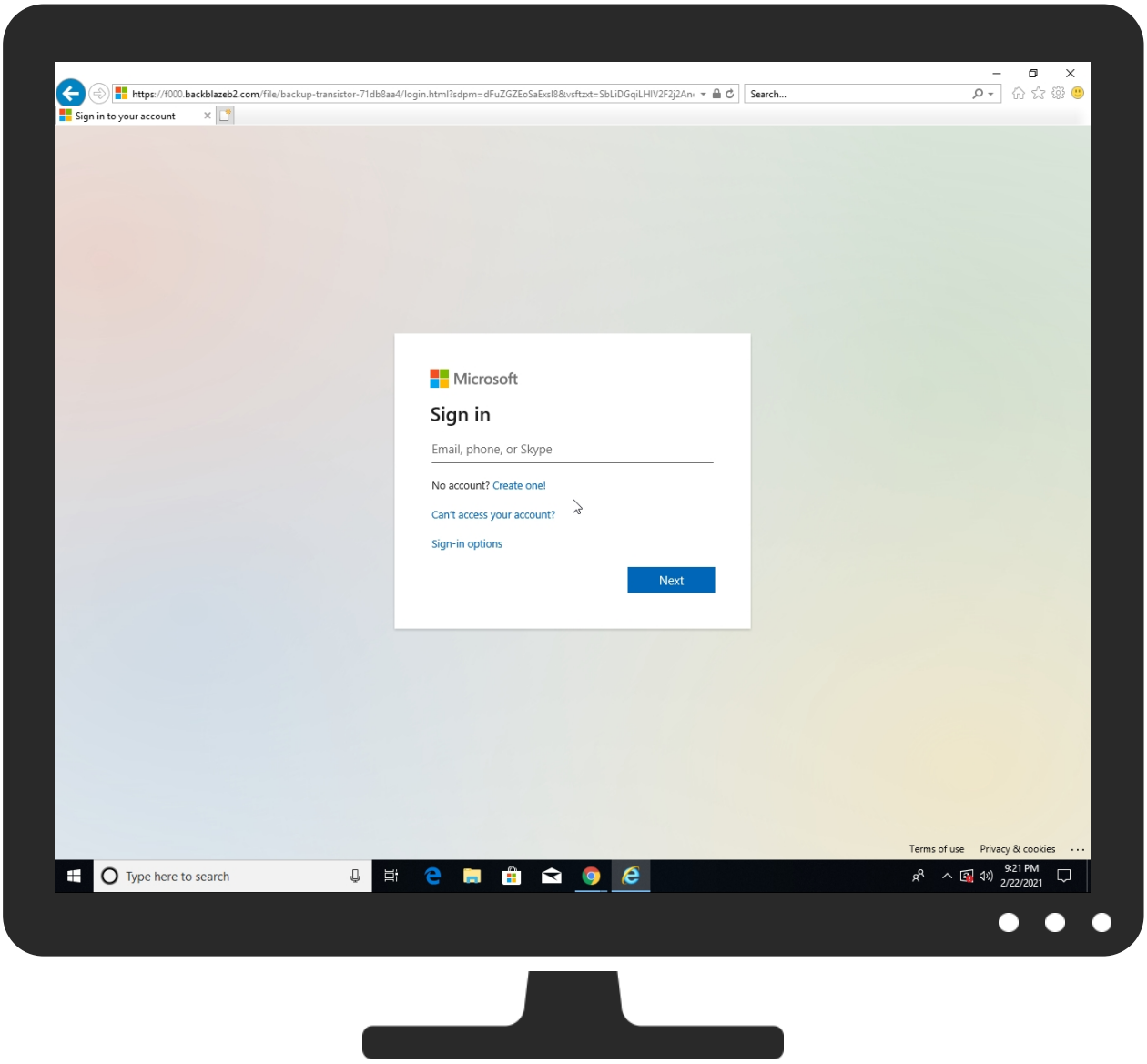


Screenshots

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
JTI NETWORK - Proposal & Quote.pdf	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
f000.backblazeb2.com	2%	Virustotal		Browse
sni1gl.wpc.alphacdn.net	0%	Virustotal		Browse
aadcdn.msauth.net	1%	Virustotal		Browse
assets.onestore.ms	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://f000.backblazeb2.com/file/backup-transistor-71db8aa4/login.html?sdpm=dFuZGZEoSaExsl8&vsftzxt=SbLiDGqiLHIV2F2j2AneQ6&sdd=fAoxPoVqMskFU49WInCIKVEYtNY2J5	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://f000.backtml$	0%	Avira URL Cloud	safe	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://www.youradchoices.ca/fr	0%	URL Reputation	safe	
http://https://ims-na1.adobelogin.comU	0%	Avira URL Cloud	safe	
http://https://f000.backblazeb2.com/file/backup-transistor-71db8aa4/index.htmlRoot	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/_	0%	Avira URL Cloud	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/a	0%	Avira URL Cloud	safe	
http://https://f000.backblazeb2.com/file/backup-transistor-71db8aa4/login.html?sdpm=dFuZRoot	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2.js?v=1	0%	URL Reputation	safe	
http://https://f000.backblazeb2.comU	0%	Avira URL Cloud	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://https://privacy.m	0%	Avira URL Cloud	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://https://aadcdn.msauth.net/shared/1.0/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c.s	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://https://f000.backblazeb2.com	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	0%	URL Reputation	safe	
http://www.mpegla.com).	0%	Avira URL Cloud	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	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	0%	URL Reputation	safe	
http://https://www.skype.com).	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2~(	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2~(	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/images/favicon.ico?v=2~(	0%	URL Reputation	safe	
http://https://f000.backblazeb2.com/file/backup-transistor-71db8aa4/login.html?sdpm=dFuZGZEoSaExsl8&vsftzxt	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://fontello.comiconsRegulariconsiconsVersion	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/shared/1.0/content/images/ellipsis_96f69d0cefd8a8ba623a182c351ccc64.png	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net/lightweightsignuppackage_OwHbS0yAbvGpBlUF0ZS3iA2.js?v=1	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net/lwsignupstringscountrybirthdate_en-us_VxjLzmQAiLRyhA2ROX72uQ2.js?v=1	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net/shared/1.0/content/images/microsoft_logo_ed9c9eb0dce17d752bedea6b5acda6d9.	0%	Avira URL Cloud	safe	
http://https://acctcdn.msauth.net	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://acctcdn.msauth.net	0%	URL Reputation	safe	
http://https://acctcdn.msauth.net	0%	URL Reputation	safe	
http://https://f000.backblazeb2.com/file/backup-transistor-71db8aa4/login.html?sdpm=dFuZ	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	0%	URL Reputation	safe	
http://www.npes.org/pdfx/ns/id/z	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	
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://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/tmp9	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net/shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.	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://f000.backblazeb2.com/file/backup-transistor-71db8aa4/login.html?sdpm=dFuZGZEoS	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net/shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.s	0%	Avira URL Cloud	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	URL Reputation	safe	
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	0%	URL Reputation	safe	
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	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://cipa.jp/exif/1.0/U	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
f000.backblazeb2.com	104.153.233.177	true	false	• 2%, Virustotal, Browse	unknown
sni1gl.wpc.alphacdn.net	152.199.21.175	true	false	• 0%, Virustotal, Browse	unknown
signup.live.com	unknown	unknown	false		high
aadcdn.msauth.net	unknown	unknown	false	• 1%, Virustotal, Browse	unknown
assets.onestore.ms	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
fpt.live.com	unknown	unknown	false		high
acctcdn.msauth.net	unknown	unknown	false		unknown
ajax.aspnetcdn.com	unknown	unknown	false		high
backblazeb2.com	unknown	unknown	false		unknown

URLs from Memory and Binaries

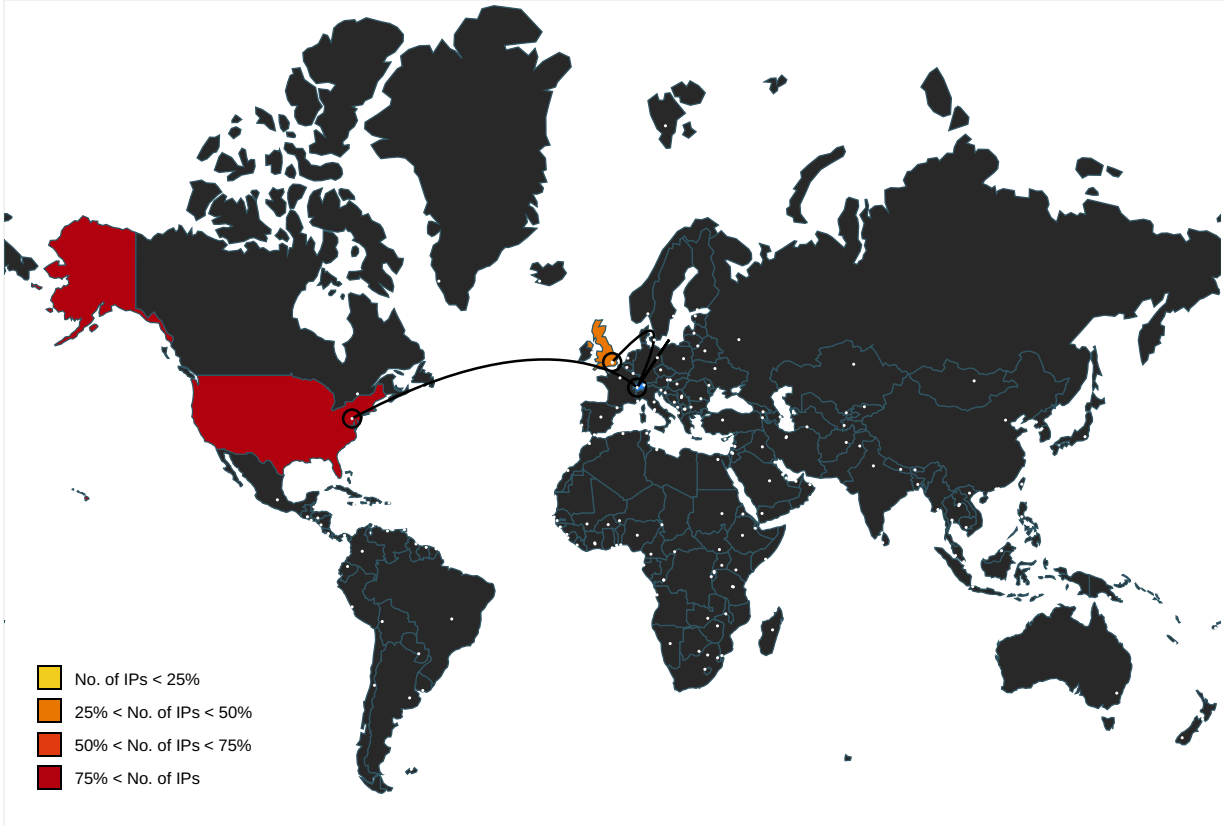
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aka.ms/useterms	servicesagreement[1].htm.25.dr	false		high
http://https://www.acuityads.com/opt-out/	privacystatement[1].htm.25.dr	false		high
http://https://f000.backtml$	{FC9A1D26-7596-11EB-90E4-ECF4BB862DED}.dat.24.dr	false	• Avira URL Cloud: safe	low
http://https://www.youradchoices.ca/fr	privacystatement[1].htm.25.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.adr.org	servicesagreement[1].htm.25.dr	false		high
http://https://ims-na1.adobelogin.comU	AcroRd32.exe, 00000002.00000002.365165579.000000000AB30000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.xbox.com/en-US/Legal/CodeOfConduct)	servicesagreement[1].htm.25.dr	false		high
http://www.asp.net/ajaxlibrary/CDN.ashx.	privacystatement[1].htm.25.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://f000.backblazeb2.com/file/backup-transistor-71db8aa4/index.htmlRoot	{FC9A1D26-7596-11EB-90E4-ECF4BB862DED}.dat.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://fpt.live.com/	QVMJZWO9.htm.25.dr	false		high
http://https://fpt.live.com/?session_id=0656ef1f3f31449c938682f87c100e08&CustomerId=33e01921-4d64-4f8c-a055	{FC9A1D26-7596-11EB-90E4-ECF4BB862DED}.dat.24.dr	false		high
http://https://www.xbox.com/en-US/Legal/CodeOfConduct	servicesagreement[1].htm.25.dr	false		high
http://opensource.org/licenses/mit-license.php)	knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2[1].js.25.dr	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/_	AcroRd32.exe, 00000002.00000002.369850470.000000000BB66000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.json.org/json2.js	knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2[1].js.25.dr	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/a	AcroRd32.exe, 00000002.00000002.369850470.000000000BB66000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://aka.ms/taxservice	servicesagreement[1].htm.25.dr	false		high
http://www.aiim.org/pdfa/ns/type#	AcroRd32.exe, 00000002.00000002.359860798.0000000009898000.00000004.00000001.sdmp	false		high
http://https://skype.com/go/myaccount	servicesagreement[1].htm.25.dr	false		high
http://https://www.skype.com	servicesagreement[1].htm.25.dr	false		high
http://https://f000.backblazeb2.com/file/backup-transistor-71db8aa4/login.html?sdpm=dFuZRoot	{FC9A1D26-7596-11EB-90E4-ECF4BB862DED}.dat.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.appnexus.com/	privacystatement[1].htm.25.dr	false		high
http://https://acctcdn.msauth.net/knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2.js?v=1	signup[1].htm.25.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://f000.backblazeb2.comU	AcroRd32.exe, 00000002.00000003.352540127.000000000BCB3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.osmf.org/drm/default	AcroRd32.exe, 00000002.00000002.355334148.0000000008000000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://privacy.m	{FC9A1D26-7596-11EB-90E4-ECF4BB862DED}.dat.24.dr	false	• Avira URL Cloud: safe	unknown
http://www.osmf.org/elementId%http://www.osmf.org/temporal/embedded$http://www.osmf.org/temporal/dyn	AcroRd32.exe, 00000002.00000002.355334148.0000000008000000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://aadcdn.msauth.net/shared/1.0/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c.s	{FC9A1D26-7596-11EB-90E4-ECF4BB862DED}.dat.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://priv-policy.imrworldwide.com/priv/browser/us/en/optout.html	privacystatement[1].htm.25.dr	false		high
http://www.reddit.com/	msapplication.xml4.24.dr	false		high
http://https://www.youronlinechoices.com/	privacystatement[1].htm.25.dr	false		high
http://https://mixer.com/contact	servicesagreement[1].htm.25.dr	false		high
http://https://www.adjust.com/opt-out/	privacystatement[1].htm.25.dr	false		high
http://ns.useplus.org/ldf/xmp/1.0/	AcroRd32.exe, 00000002.00000002.359860798.0000000009898000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://f000.backblazeb2.com	AcroRd32.exe, 00000002.00000002.369879174.000000000BB7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.xbox.com/managedatacollection	privacystatement[1].htm.25.dr	false		high
http://https://www.xbox.com/legal/codeofconduct	privacystatement[1].htm.25.dr	false		high
http://https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	signup[1].htm.25.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.mpegla.com).	servicesagreement[1].htm.25.dr	false	• Avira URL Cloud: safe	low
http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/	AcroRd32.exe, 00000002.00000002.359860798.0000000009898000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://aka.ms/kinectprivacy/	privacystatement[1].htm.25.dr	false		high
http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1	signup[1].htm.25.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.skype.com).	servicesagreement[1].htm.25.dr	false	• Avira URL Cloud: safe	low
http://https://www.xbox.com	privacystatement[1].htm.25.dr	false		high
http://https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protectio	privacystatement[1].htm.25.dr	false		high
http://https://github.com/douglascrockford/JSON-js	signup[1].htm.25.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://acctcdn.msauth.net/images/favicon.ico?v=2~(	imagestore.dat.25.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://f000.backblazeb2.com/file/backup-transistor-71db8aa4/login.html?sdpm=dFuZGZEoSaExsl8&vsftzxt	{FC9A1D26-7596-11EB-90E4-ECF4BB862DED}.dat.24.dr, ~DF1CCBA7FC635E4D8F.TMP.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1	signup[1].htm.25.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.opensource.org/licenses/mit-license.php)	knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2[1].js.25.dr	false		high
http://fontello.comiconsRegulariconsiconsVersion	icons[1].eot.25.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://aadcdn.msauth.net/shared/1.0/content/images/ellipsis_96f69d0cefd8a8ba623a182c351ccc64.png	{FC9A1D26-7596-11EB-90E4-ECF4BB862DED}.dat.24.dr	false	• Avira URL Cloud: safe	unknown
http://www.youtube.com/	msapplication.xml7.24.dr	false		high
http://https://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html	privacystatement[1].htm.25.dr	false		high
http://https://www.skype.com/go/legal	servicesagreement[1].htm.25.dr	false		high
http://https://mixer.com/about/tos	servicesagreement[1].htm.25.dr	false		high
http://https://fpt.live.com/?session_id=b58882512b7c40d78c42f4d88f1affac&CustomerId=33e01921-4d64-4f8c-a055	{FC9A1D26-7596-11EB-90E4-ECF4BB862DED}.dat.24.dr	false		high
http://https://www.linkedin.com/legal/privacy-policy	privacystatement[1].htm.25.dr	false		high
http://https://ims-na1.adobelogin.com	AcroRd32.exe, 00000002.00000002.365165579.000000000AB30000.00000004.00000001.sdmp	false		high
http://https://aadcdn.msauth.net	{FC9A1D26-7596-11EB-90E4-ECF4BB862DED}.dat.24.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://acctcdn.msauth.net/lightweightsignuppackage_OwHbS0yAbvGpBlUF0ZS3iA2.js?v=1	signup[1].htm.25.dr	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/DPA	privacystatement[1].htm.25.dr	false		high
http://https://support.xbox.com/help/friends-social-activity/community/use-safety-settings	privacystatement[1].htm.25.dr	false		high
http://https://www.xbox.com/Legal/ThirdPartyDataSharing	privacystatement[1].htm.25.dr	false		high
http://https://acctcdn.msauth.net/lwsignupstringscountrybirthdate_en-us_VxjLzmQAiLRyhA2ROX72uQ2.js?v=1	signup[1].htm.25.dr	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/redeemrewards	servicesagreement[1].htm.25.dr	false		high
http://https://signin.kissmetrics.com/privacy/#controls	privacystatement[1].htm.25.dr	false		high
http://https://login.skype.com/login	privacystatement[1].htm.25.dr	false		high
http://https://www.skype.com/go/ustax	servicesagreement[1].htm.25.dr	false		high
http://jquery.org/license	jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2[1].js.25.dr	false		high
http://https://aadcdn.msauth.net/shared/1.0/content/images/microsoft_logo_ed9c9eb0dce17d752bedea6b5acda6d9.	{FC9A1D26-7596-11EB-90E4-ECF4BB862DED}.dat.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://acctcdn.msauth.net	signup[1].htm.25.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://f000.backblazeb2.com/file/backup-transistor-71db8aa4/login.html?sdpm=dFuZ	{FC9A1D26-7596-11EB-90E4-ECF4BB862DED}.dat.24.dr	false	• Avira URL Cloud: safe	unknown
http://www.aiim.org/pdfa/ns/id/a	AcroRd32.exe, 00000002.00000002.365165579.000000000AB30000.00000004.00000001.sdmp	false		high
http://https://www.optimizely.com/legal/opt-out/	privacystatement[1].htm.25.dr	false		high
http://www.aiim.org/pdfa/ns/schema#	AcroRd32.exe, 00000002.00000002.359860798.0000000009898000.00000004.00000001.sdmp	false		high
http://sizzlejs.com/	jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2[1].js.25.dr	false		high
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~(	imagestore.dat.25.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.npes.org/pdfx/ns/id/z	AcroRd32.exe, 00000002.00000002.365165579.000000000AB30000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.osmf.org/region/target#http://www.osmf.org/layout/renderer#http://www.osmf.org/layout/abs	AcroRd32.exe, 00000002.00000002.355334148.0000000008000000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/tmp9	AcroRd32.exe, 00000002.00000002.369850470.000000000BB66000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://aadcdn.msauth.net/shared/1.0/content/images/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.	{FC9A1D26-7596-11EB-90E4-ECF4BB862DED}.dat.24.dr	false	• Avira URL Cloud: safe	unknown
http://www.amazon.com/	msapplication.xml.24.dr	false		high
http://cipa.jp/exif/1.0/	AcroRd32.exe, 00000002.00000002.365165579.000000000AB30000.00000004.00000001.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, 00000002.00000002.355334148.0000000008000000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://signup.live.com/error.aspx?errcode=1045&mkt=en-US	signup[1].htm.25.dr	false		high
http://https://login.windows-ppe.net	Me[1].htm.25.dr	false		high
http://www.twitter.com/	msapplication.xml5.24.dr	false		high
http://https://f000.backblazeb2.com/file/backup-transistor-71db8aa4/login.html?sdpm=dFuZGZEoS	{FC9A1D26-7596-11EB-90E4-ECF4BB862DED}.dat.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.privacyshield.gov/welcome	privacystatement[1].htm.25.dr	false		high
http://https://login.microsoftonline.com	Me[1].htm.25.dr	false		high
http://https://ondemand.webtrends.com/support/optout.asp	privacystatement[1].htm.25.dr	false		high
http://https://www.skype.com/go/legal.broadcast	servicesagreement[1].htm.25.dr	false		high
http://https://aadcdn.msauth.net/shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.s	{FC9A1D26-7596-11EB-90E4-ECF4BB862DED}.dat.24.dr	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico~	imagestore.dat.25.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.appsflyer.com/optout	privacystatement[1].htm.25.dr	false		high
http://https://PrefSyncJob/com.adobe.acrobat.ADotCom/Resource/Sync/Upload/	AcroRd32.exe, 00000002.00000002.369850470.000000000BB66000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.npes.org/pdfx/ns/id/	AcroRd32.exe, 00000002.00000002.365165579.000000000AB30000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://aka.ms/redeemrewards).	servicesagreement[1].htm.25.dr	false		high
http://cipa.jp/exif/1.0/U	AcroRd32.exe, 00000002.00000002.365165579.000000000AB30000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Copyright null 2021

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.153.233.177	unknown	United States		32354	UNWIREDUS	false
152.199.21.175	unknown	United States		15133	EDGECASTUS	false
80.0.0.0	unknown	United Kingdom		5089	NTLGB	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356294
Start date:	22.02.2021
Start time:	21:19:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	JTI NETWORK - Proposal & Quote.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:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.phis.winPDF@19/117@11/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Copyright null 2021

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 • Browsing link: https://login.live.com/oauth20_authorize.srf?response_type=code&client_id=51483342-085c-4d86-bf88-cf50c7252078&scope=openid+profile+email+offline_access&response_mode=form_post&redirect_uri=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2ffederation%2foauth2&state=rQIIAeNisNLJKCkpKLbS1y_ILypJzNHLzUwuyi_OTyvJz8vJzEvVS87P1csvSs9MAbGKhLgE5N-HsRnaz3GZ3Nb0o0aAj2MWI2d8TmYZWOUqRmXCxulfYGR8wch4i0nQvyjdMyW82C01JbUosSQzP-8Ci8ArFh4DZisODi4BBgkGBYYfLIyLWIG2Rik0X16_dbXTrqAUuYQeZ4ZTrPpRVd4W-b7mmV4ppv5hlW6-lqaluRYWHrl5XtppBkXhQUUhmQElZWVGAaGBtqZWhhPYhCawMZ1iY_jAxtjBznCAk_EWl4iRgaGlroGRroGJgoGllZGRlbFRFAA1&estsfed=1&uaid=0656ef1f3f31449c938682f87c100e08&signup=1&lw=1&fl=easi2&fci=https%3a%2f%2fportal.microsoftonline.com.orgid.com • Browsing link: https://login.live.com/oauth20_authorize.srf?response_type=code&client_id=51483342-085c-4d86-bf88-cf50c7252078&scope=openid+profile+email+offline_access&response_mode=form_post&redirect_uri=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2ffederation%2foauth2&state=rQIIAYWSO2_TUABG47QNtOItBsSAOjAgkNPre_2IlyHhxEmTJo7zsOvYi2UnfuVhp44dOxETLAxIMHeDASFgQiAhJuZKSGwgFlbEhBADGxT-AMsZvjN-Z-sEnafzIA-urxF5oniVRCRlMCaLswaNcJIlAG6QkMYRhWgEATGkAAovbJ3r3Ln3-vaNj7ful35-enD594tDbFOfeAsrPwimz7ArbhTN5sWdnSRJ8oFte4N_Ymdi-EPPd95g2AcM-4phh9kNy8fl3rPsnEYMoliaoQjAQAhZAPOaJKQqFBJR4iJ1KhCaB4CqqGlTqRxv9UjY7U4E2lHirjbV-EEiKDJqKfVUU4RIHe176hIAUVGXTclJRd6JBF6AmqQSrdE4EVZ19Dl7VuTiyIV_EYTeyvqR3bSDcKrPgnl0uPY8u-rOO6bqr6yewFMsQxpdvxFynE60XbO7X476HjoQpm7VWUbGEmdDhtGjJVUd9GtKXA_50N3nwiBI-0bS7uEHtNloIFtjRE8WNrk7phdWrU3ynGkoiRn4U9mMyWadcZqGw1eVAy2lR31aTkVN1r1-OeCFg2QRJAnpkIzKOMG8AyaVVVreowg9xR2Zr01hEzfnfBssxwHuV0BvIboDJwVwUGuMQ8ZxZcEsN1m9MEQFX5NGQ6XJeWy1W2qD0mxhU4G9VyposYuq3WTVUHflhSXLZivq-a4y5-KJgNdQFDsMO7SYZm1UsyS0KnE62ZMKtPNyLXf88DTwj9bOBDPL94bbszCwvYn1YR37tn7qZO5c7lJmO3PtljjzaxZ17vHEc0dP3XzbY5ZPy3UekHcmvMkcbOyq_Qou-VQFSTE3SAjKBMqLL7mxPrcRLUYyHHdZGzn4dAO4mUSQe5rCHudxR7nyd11sVqSdxLZ7r8lAH33PYvROZt5v_SfHz1kUIIMABixPMNgRFgihSQHt3OvMH0&estsfed=1&uaid=b58882512b7c40d78c42f4d88f1affac&signup=1&lw=1&fl=easi2&fci=4345a7b9-9a63-4910-a426-35363201d503&mkt=en-US • Browsing link: https://www.microsoft.com/en-US/servicesagreement/ • Browsing link: https://privacy.microsoft.com/en-US/privacystatement
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe,

conhost.exe, WmiPrvSE.exe, svchost.exe, UsoClient.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 52.147.198.201, 104.43.139.144, 104.43.193.48, 13.88.21.125, 168.61.161.212, 23.32.238.129, 23.32.238.123, 23.32.238.113, 184.30.20.134, 51.104.144.132, 23.57.80.111, 20.54.26.129, 88.221.62.148, 92.122.213.247, 92.122.213.194, 13.107.246.19, 13.107.213.19, 142.250.186.138, 40.126.31.141, 40.126.31.137, 40.126.31.8, 40.126.31.6, 40.126.31.143, 20.190.159.138, 40.126.31.4, 40.126.31.139, 13.107.42.22, 152.199.19.161, 51.104.139.180, 104.46.7.117, 52.114.20.18, 184.30.21.171, 92.122.213.201, 23.57.80.253, 152.199.19.160, 104.108.38.107
- Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, assets.onestore.ms.edgekey.net, www.tm.lg.prod.aadmsa.akadns.net, e13678.dscb.akamaiedge.net, browser.events.data.trafficmanager.net, fs-wildcard.microsoft.com.edgekey.net, acroipm2.adobe.com, a1945.g2.akamai.net, e11290.dspg.akamaiedge.net, www.microsoft.com-c-3.edgekey.net, login.live.com, star-azurefd-prod.trafficmanager.net, a122.dscd.akamai.net, www-bing-com.dual-a-0001.a-msedge.net, statics-marketingsites-eus-ms-com.akamaized.net, watson.telemetry.microsoft.com, acctcdnvzeuno.azureedge.net, acctcdnvzeuno.ec.azureedge.net, www.bing.com, e10583.dspg.akamaiedge.net, fpt2.microsoft.com, fs.microsoft.com, dual-a-0001.a-msedge.net, acroipm2.adobe.com.edgesuite.net, aadcdnoriginwus2.azureedge.net, ajax.googleapis.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, www.tm.a.prd.aadg.akadns.net, assets.onestore.ms.akadns.net, skypedataprdcolcus15.cloudapp.net, c-s.cms.ms.akadns.net, ris.api.iris.microsoft.com, ssl.adobe.com.edgekey.net, skypedataprdcolaus02.cloudapp.net, t-0009.t-msedge.net, blobcollector.events.data.trafficmanager.net, account.msa.akadns6.net, aadcdnoriginwus2.afd.azureedge.net, c.s-microsoft.com-c.edgekey.net, greenid-production.eastus2.cloudapp.azure.com, privacy.microsoft.com.edgekey.net, fpt.microsoft.com, cs9.wpc.v0cdn.net, e4578.dscb.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, acctcdn.trafficmanager.net, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, iecvlist.microsoft.com, go.microsoft.com, mscomajax.vo.msecnd.net, dual.t-0009.t-msedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, ie9comview.vo.msecnd.net, cs22.wpc.v0cdn.net, e1723.g.akamaiedge.net, star-azureedge-prod.trafficmanager.net, greenidvnext-prod.trafficmanager.net, login.msa.msidentity.com, skypedataprdcoleus16.cloudapp.net, browser.events.data.microsoft.com, c.s-microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, armmf.adobe.com, privacy.microsoft.com, go.microsoft.com.edgekey.net, l-0013.l-msedge.net, e13678.dscg.akamaiedge.net, skypedataprdcolwus15.cloudapp.net, www.microsoft.com, e13678.dspb.akamaiedge.net, wcpstatic.microsoft.com
- 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 NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:20:34	API Interceptor	11x Sleep call for process: RdrCEF.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
152.199.21.175	http://https://u.to/r9nvGQ	Get hash	malicious	Browse	• s.c.dk/fonts/yousee-iconfont.woff
	http://cdn2.driversupport.com/dsone/gppc_ds1/DSOne.exe	Get hash	malicious	Browse	• cdn2.driversupport.com/dsone/gppc_ds1/DSOneApp.exe
	http://cdn2.driversupport.com/dsone/gdn_ds1/DSOne.exe	Get hash	malicious	Browse	• cdn2.driversupport.com/dsone/gdn_ds1/DSOneApp.exe
104.153.233.177	#U266b Audio_47720.wavv - - Copy.htm	Get hash	malicious	Browse	
	http://https://protect-eu.mimecast.com/s/pcV8CNOoQcNB43Vcm17QZ?domain=watsonbatty-my.sharepoint.com	Get hash	malicious	Browse	
	http://https://f000.backblazeb2.com/file/url-datasecured-k20c065aadbcsjhdcbjs/1uyhchduiahc/index.html	Get hash	malicious	Browse	
	http://https://f000.backblazeb2.com/file/url-data-web-storage-secured-56adbcsjhdcbjs/web-data-server-1uyhchduiahc/index.html	Get hash	malicious	Browse	
	http://https://f000.backblazeb2.com/file/url-data-web-storage-secured-56adbcsjhdcbjs/web-data-server-1uyhchduiahc/index.html	Get hash	malicious	Browse	
	http://https://f000.backblazeb2.com/file/url-data-web-storage-secured-56adbcsjhdcbjs/web-data-server-1uyhchduiahc/index.html&data=04|01||a6737981c3be4cd5de8c08d8b18a51e0|84df9e7fe9f640afb435aaaaaaaaaaaa|1|0|637454554918925175|Unknown|TWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJ	Get hash	malicious	Browse	
	http://https://secureddoc.unicornplatform.com	Get hash	malicious	Browse	
	http://https://f000.backblazeb2.com/file/amalgamization1053/index.html	Get hash	malicious	Browse	
	http://https://f000.backblazeb2.com/file/progenitress3434436/index.html	Get hash	malicious	Browse	
	http://https://secureddoc.unicornplatform.com/	Get hash	malicious	Browse	
	http://https://secureddoc.unicornplatform.com	Get hash	malicious	Browse	
	http://https://f000.backblazeb2.com/file/url-data-web-storage-secured-c001x1zvcykky52351/web-data-server-uid-space-cloud-loctation-dmoain-number-server-linux-maxutf-uuid-no-30m40a2qcokk3e86/index.html	Get hash	malicious	Browse	
	http://https://f000.backblazeb2.com/file/url-data-web-storage-secured-13351212/web-data-server-uid-space-cloud-loctation-dmoain-number-server-linux-maxutf-uuid-no-1864395359/index.html#martien.janssen@rivm.nl	Get hash	malicious	Browse	
80.0.0.0	2021-02-15__Mail-Degroof-Petercam_ENC.docx	Get hash	malicious	Browse	
	InformaAllSecure_Enhanced_Health_Safety_Standards_2021.docm	Get hash	malicious	Browse	
	Swift.pdf.jar	Get hash	malicious	Browse	
	0001.jar	Get hash	malicious	Browse	
	FedEx-Shipment-90161131174.jar	Get hash	malicious	Browse	
	FedEx-Shipment-61821461149.jar	Get hash	malicious	Browse	
	FedEx-Shipment-8161131174.jar	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	agenciatributaria5668.vbs	Get hash	malicious	Browse	
	Statement for T10495.jar	Get hash	malicious	Browse	
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	
	TREKSTA 2021 Business Plan..exe	Get hash	malicious	Browse	
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	
	2EB0.tmp.exe	Get hash	malicious	Browse	
	muddydoc.exe	Get hash	malicious	Browse	
	RQMofd68Ad.exe	Get hash	malicious	Browse	
	http://https://awattorneys-my.sharepoint.com/:b:/p/fgalante/EcRfEpzLM_tOh_Roewbwm9oB4JarWh_30QaPZLGUdNbnuw?e=4%3aqmwocp&at=9	Get hash	malicious	Browse	
	http://quickneasyrecipes.co	Get hash	malicious	Browse	
	http://https://dck12-my.sharepoint.com:443/:b:/g/personal/tanya_mckelvin_k12_dc_gov/EbGhLtD47K1Cl18cC--Ad0sBxiRFwsui9s7PYb2eA-FMZg?e=4%3arCBWhd&at=9__;JQ!!P4oOa0cl!xjyiOci-WnHuSljf0v9YP9XHTo1mHg1DdlnrlGItn8ysOUKeJHjzL7gjiYG6nZ8pLQ$	Get hash	malicious	Browse	
	http://https://public.3.basecamp.com/p/2D4prniZtSHtN5Qfx4XocXX3	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
f000.backblazeb2.com	#U266b Audio_47720.wavv - - Copy.htm	Get hash	malicious	Browse	• 104.153.233.177
	http://https://protect-eu.mimecast.com/s/pcV8CNOoQcNB43Vcm17QZ?domain=watsonbatty-my.sharepoint.com	Get hash	malicious	Browse	• 104.153.233.177
	http://https://f000.backblazeb2.com/file/url-datasecured-k20c065aadbcsjhdcbjs/1uyhchduiahc/index.html	Get hash	malicious	Browse	• 104.153.233.177
	http://https://f000.backblazeb2.com/file/url-data-web-storage-secured-56adbcsjhdcbjs/web-data-server-1uyhchduiahc/index.html	Get hash	malicious	Browse	• 104.153.233.177
	http://https://f000.backblazeb2.com/file/url-data-web-storage-secured-56adbcsjhdcbjs/web-data-server-1uyhchduiahc/index.html	Get hash	malicious	Browse	• 104.153.233.177
	http://https://f000.backblazeb2.com/file/url-data-web-storage-secured-56adbcsjhdcbjs/web-data-server-1uyhchduiahc/index.html&data=04|01||a6737981c3be4cd5de8c08d8b18a51e0|84df9e7fe9f640afb435aaaaaaaaaaaa|1|0|637454554918925175|Unknown|TWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJ	Get hash	malicious	Browse	• 104.153.233.177
	http://https://secureddoc.unicornplatform.com	Get hash	malicious	Browse	• 104.153.233.177
	http://https://f000.backblazeb2.com/file/amalgamization1053/index.html	Get hash	malicious	Browse	• 104.153.233.177
	http://https://f000.backblazeb2.com/file/progenitress3434436/index.html	Get hash	malicious	Browse	• 104.153.233.177
	http://https://secureddoc.unicornplatform.com/	Get hash	malicious	Browse	• 104.153.233.177
	http://https://secureddoc.unicornplatform.com	Get hash	malicious	Browse	• 104.153.233.177
	http://https://f000.backblazeb2.com/file/url-data-web-storage-secured-c001x1zvcykky52351/web-data-server-uid-space-cloud-loctation-dmoain-number-server-linux-maxutf-uuid-no-30m40a2qcokk3e86/index.html	Get hash	malicious	Browse	• 104.153.233.177
	http://https://f000.backblazeb2.com/file/url-data-web-storage-secured-13351212/web-data-server-uid-space-cloud-loctation-dmoain-number-server-linux-maxutf-uuid-no-1864395359/index.html#martien.janssen@rivm.nl	Get hash	malicious	Browse	• 104.153.233.177
	http://https://f000.backblazeb2.com/file/jha-0086/copyab.html	Get hash	malicious	Browse	• 162.244.62.197
sni1gl.wpc.alphacdn.net	Remittance58404.htm	Get hash	malicious	Browse	• 152.199.21.175
	#U266b Audio_47720.wavv - - Copy.htm	Get hash	malicious	Browse	• 152.199.21.175
	INVOICES & STATEMENTS_02201.htm	Get hash	malicious	Browse	• 152.199.21.175
	http://https://r0qp15r0b1rq05rrpbqbrpq5.s3-eu-west-1.amazonaws.com/Ap3dX.html#joetorre@gmail.com	Get hash	malicious	Browse	• 152.199.21.175
	http://https://r0qp15r0b1rq05rrpbqbrpq5.s3-eu-west-1.amazonaws.com/Ap3dX.html#orderadmin@roku.com	Get hash	malicious	Browse	• 152.199.21.175
	http://https://blog.dericoin.com/wp-includes/shell/ivd/Office/office/voicemail/index.php	Get hash	malicious	Browse	• 152.199.21.175

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://dfc0cfdf90fq0d0090q00cdc.ams3.cdn.digitaloceanspaces.com/index.html	Get hash	malicious	Browse	• 152.199.21.175
	http://https://f000.backblazeb2.com/file/url-datasecured-k20c065aadbcsjhdcbjs/1uyhchduiahc/index.html	Get hash	malicious	Browse	• 152.199.21.175
	Westernsouthernlife8PG5-YSGL2K-TVU4.htm	Get hash	malicious	Browse	• 152.199.21.175
	http://https://grantsvillemd.xyz/amlsbC5tY2dydWRlckB3ZXN0ZXJuc291dGhlcm4uY29t	Get hash	malicious	Browse	• 152.199.21.175
	Audio_47720.wavv - - Copy.htm	Get hash	malicious	Browse	• 152.199.21.175
	#Ud83d#Udcdejsi12615.html	Get hash	malicious	Browse	• 152.199.21.175
	http://https://omoolowo001.github.io/myfirstrepo/YWNjb3VudHNfbG9nindex.html?scriptID=35662936635352205&cookies=MC4xOTUyNjY0OTg0MzM0NTQ0NQ&token=81117470799998&email=jeaton@nlcmutual.com	Get hash	malicious	Browse	• 152.199.21.175
	http://https://fultonmv.github.io/amanadpsoptodresi/aru.html?bbre=do9348wesid	Get hash	malicious	Browse	• 152.199.21.175
	http://https://rzh09.github.io/kirapzoxda/adiuew.html?bbre=as83wsdcx	Get hash	malicious	Browse	• 152.199.21.175
	http://https://flcfm.com/sign-on.ce9876/365txt	Get hash	malicious	Browse	• 152.199.21.175
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fseacoccs.github.io%2fvivapdeltoozx%2fsorirw.html%3fbbre%3dod948reids&c=E,1,vSy_DaxVlhDKTU_DAd4XDQRKFbpEz58IBL3G2ibxtXxy4isfCn6tn5y2D7KvyG8o1RL3a--vpSQ8W1tCBVf3nGFmVP0O8ZI4kUultyRSb1120A,,&typo=1	Get hash	malicious	Browse	• 152.199.21.175
	http://https://conrad805.github.io/vkiapdeijxzix/uead.html?bbre=ds94refszx	Get hash	malicious	Browse	• 152.199.21.175
	http://https://oncqooractlboiig-dot-tundasma.el.r.appspot.com/#ronan.oconnor@cignal.ie	Get hash	malicious	Browse	• 152.199.21.175
	http://https://laborergenetic.com/page/2020/	Get hash	malicious	Browse	• 152.199.21.175

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EDGECASTUS	FAX-MESSAGE201636576736375362.hTMl	Get hash	malicious	Browse	• 152.199.23.37
	Z4fYo3NwC0.exe	Get hash	malicious	Browse	• 93.184.220.29
	602b97e0b415b.png.dll	Get hash	malicious	Browse	• 192.229.221.215
	Thursday, February 11th, 2021, 20210211033346.3BD4A181171AEBE1@gotasdeamor.cl.htm	Get hash	malicious	Browse	• 152.199.23.37
	Tuesday, February 9th, 2021 8%3A1%3A54 a.m., _20210209080154.8E45EAA12FF8DC21@sophiajoyas.cl_.html	Get hash	malicious	Browse	• 192.229.221.185
	Farie PO.doc	Get hash	malicious	Browse	• 192.229.221.185
	5DktGbEvIA.apk	Get hash	malicious	Browse	• 68.232.34.193
	February Payroll.xls.htm	Get hash	malicious	Browse	• 152.199.23.37
	Tuesday, February 9th, 2021 83422 a.m., 20210209083422.7B8380338EC1D61B@sophiajoyas.cl.html	Get hash	malicious	Browse	• 152.199.23.37
	Friday_ February 5th_ 2021 64427 a.m._ 20210205064427.64791275BD060468@juidine.com.html	Get hash	malicious	Browse	• 192.229.221.185
	Remittance58404.htm	Get hash	malicious	Browse	• 152.199.21.175
	Thursday, February 4th, 2021 103440 p.m., 20210204223440.464D4D4AD1BFDE50@juidine.com.html	Get hash	malicious	Browse	• 152.199.23.37
	Curriculo Laura Sperandio.xlsm	Get hash	malicious	Browse	• 152.199.19.161
	#U266b Audio_47720.wavv - - Copy.htm	Get hash	malicious	Browse	• 152.199.21.175
	RA test.docx	Get hash	malicious	Browse	• 152.199.21.141
	Rolled Alloys Possible Infection.docx	Get hash	malicious	Browse	• 192.229.233.50
	PAYMENT.xlsx	Get hash	malicious	Browse	• 152.199.23.37
	PAYMENT INFO.xlsx	Get hash	malicious	Browse	• 152.199.23.37
	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	• 152.199.23.72
	1_25_2021 11_20_30 a.m., [Payment 457 CMSupportDev].html	Get hash	malicious	Browse	• 152.199.23.37
UNWIREDUS	#U266b Audio_47720.wavv - - Copy.htm	Get hash	malicious	Browse	• 104.153.233.177
	http://https://protect-eu.mimecast.com/s/pcV8CNOoQcNB43Vcm17QZ?domain=watsonbatty-my.sharepoint.com	Get hash	malicious	Browse	• 104.153.233.177
	http://https://f000.backblazeb2.com/file/url-datasecured-k20c065aadbcsjhdcbjs/1uyhchduiahc/index.html	Get hash	malicious	Browse	• 104.153.233.177

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://f000.backblazeb2.com/file/url-data-web-storage-secured-56adbcsjhdcbjs/web-data-server-1uyhchduiahc/index.html	Get hash	malicious	Browse	• 104.153.233.177
	http://https://f000.backblazeb2.com/file/url-data-web-storage-secured-56adbcsjhdcbjs/web-data-server-1uyhchduiahc/index.html	Get hash	malicious	Browse	• 104.153.233.177
	http://https://f000.backblazeb2.com/file/url-data-web-storage-secured-56adbcsjhdcbjs/web-data-server-1uyhchduiahc/index.html&data=04|01||a6737981c3be4cd5de8c08d8b18a51e0|84df9e7fe9f640afb435aaaaaaaaaaaa|1|0|637454554918925175|Unknown|TWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJ	Get hash	malicious	Browse	• 104.153.233.177
	http://https://secureddoc.unicornplatform.com	Get hash	malicious	Browse	• 104.153.233.177
	http://https://f000.backblazeb2.com/file/amalgamization1053/index.html	Get hash	malicious	Browse	• 104.153.233.177
	http://https://f000.backblazeb2.com/file/progenitress3434436/index.html	Get hash	malicious	Browse	• 104.153.233.177
	http://https://secureddoc.unicornplatform.com/	Get hash	malicious	Browse	• 104.153.233.177
	http://https://secureddoc.unicornplatform.com	Get hash	malicious	Browse	• 104.153.233.177
	http://https://f000.backblazeb2.com/file/url-data-web-storage-secured-c001x1zvcykky52351/web-data-server-uid-space-cloud-loctation-dmoain-number-server-linux-maxutf-uuid-no-30m40a2qcokk3e86/index.html	Get hash	malicious	Browse	• 104.153.233.177
	http://https://f000.backblazeb2.com/file/url-data-web-storage-secured-13351212/web-data-server-uid-space-cloud-loctation-dmoain-number-server-linux-maxutf-uuid-no-1864395359/index.html#martien.janssen@rivm.nl	Get hash	malicious	Browse	• 104.153.233.177
	#Ud83d#Udcdevoice-message-733_254590.htm	Get hash	malicious	Browse	• 206.190.215.16
	#Ud83d#UdcdeAudio_Message-374672_1013.htm	Get hash	malicious	Browse	• 206.190.215.16
	http://https://f000.backblazeb2.com/file/jha-0086/copyab.html	Get hash	malicious	Browse	• 162.244.62.197
NTLGB	2021-02-15__Mail-Degroof-Petercam_ENC.docx	Get hash	malicious	Browse	• 80.0.0.0
	InformaAllSecure_Enhanced_Health_Safety_Standards_2021.docm	Get hash	malicious	Browse	• 80.0.0.0
	kF1JPCXvSq.dll	Get hash	malicious	Browse	• 82.12.157.95
	wEcncyxrEe	Get hash	malicious	Browse	• 213.48.143.199
	Swift.pdf.jar	Get hash	malicious	Browse	• 80.0.0.0
	0001.jar	Get hash	malicious	Browse	• 80.0.0.0
	FedEx-Shipment-90161131174.jar	Get hash	malicious	Browse	• 80.0.0.0
	FedEx-Shipment-61821461149.jar	Get hash	malicious	Browse	• 80.0.0.0
	FedEx-Shipment-8161131174.jar	Get hash	malicious	Browse	• 80.0.0.0
	agenciatributaria5668.vbs	Get hash	malicious	Browse	• 80.0.0.0
	Statement for T10495.jar	Get hash	malicious	Browse	• 80.0.0.0
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	• 80.0.0.0
	TREKSTA 2021 Business Plan..exe	Get hash	malicious	Browse	• 80.0.0.0
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	SPEPAY13012021-20-00000009.pdf.exe	Get hash	malicious	Browse	• 80.0.0.0
	2EB0.tmp.exe	Get hash	malicious	Browse	• 80.0.0.0
	muddydoc.exe	Get hash	malicious	Browse	• 80.0.0.0
	RQMofd68Ad.exe	Get hash	malicious	Browse	• 80.0.0.0
	http://https://awattorneys-my.sharepoint.com/:b:/p/fgalante/EcRfEpzLM_tOh_Roewbwm9oB4JarWh_30QaPZLGUdNbnuw?e=4%3aqmwocp&at=9	Get hash	malicious	Browse	• 80.0.0.0
	http://quickneasyrecipes.co	Get hash	malicious	Browse	• 80.0.0.0

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	rieuro.dll	Get hash	malicious	Browse	• 152.199.21.175
	receipt145.htm	Get hash	malicious	Browse	• 152.199.21.175
	One Note shergott@vivaldicap.com.html	Get hash	malicious	Browse	• 152.199.21.175
	FAX-MESSAGE201636576736375362.hTMl	Get hash	malicious	Browse	• 152.199.21.175
	message_zdm (2).html	Get hash	malicious	Browse	• 152.199.21.175
	Small Charities.xlsx	Get hash	malicious	Browse	• 152.199.21.175
	leaseplan-invoice-831008_xls2.HtMl	Get hash	malicious	Browse	• 152.199.21.175
	7lM8HxwfAm.dll	Get hash	malicious	Browse	• 152.199.21.175
	LcA7GaqAXC.dll	Get hash	malicious	Browse	• 152.199.21.175

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	4FHOFKHnX8.dll	Get hash	malicious	Browse	• 152.199.21.175
	5N5yxttthP.dll	Get hash	malicious	Browse	• 152.199.21.175
	vBKmtJ58Eo.dll	Get hash	malicious	Browse	• 152.199.21.175
	5293ea9467ea45e928620a5ed74440f5.exe	Get hash	malicious	Browse	• 152.199.21.175
	f1a14e6352036833f1c109e1bb2934f2.exe	Get hash	malicious	Browse	• 152.199.21.175
	Njs4kjnD5X.dll	Get hash	malicious	Browse	• 152.199.21.175
	Uiha1GUS7S.dll	Get hash	malicious	Browse	• 152.199.21.175
	SecuriteInfo.com.Mal.EncPk-APW.20360.dll	Get hash	malicious	Browse	• 152.199.21.175
	10.dll	Get hash	malicious	Browse	• 152.199.21.175
	iopjvdf.dll	Get hash	malicious	Browse	• 152.199.21.175
	d88e07467ddcf9e3b19fa972b9f000d1.exe	Get hash	malicious	Browse	• 152.199.21.175

Dropped Files

No context

Created / dropped Files

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):	820
Entropy (8bit):	5.69142111947114
Encrypted:	false
SSDEEP:	12:vDRM9myIVZiEMDRM9cZiE4DRM9qMbZiE3DRM9fZiE:7+E6MEeaEEzNE
MD5:	5CBE0C39449F70619C621E65972BE213
SHA1:	D9CE54C0EDD83A04B8159C190B4980A7B55F40DB
SHA-256:	5547F36DA315A1EAACCD4785FF688D153993B234243C438A3671170F805F8892
SHA-512:	993196EB0F8BC1B7DADF86DBB2BF6188276E997590E65AA9546429078FF1B8895897617DF61A6AA7D1EF49E3197C6634E94047128E1988BBB52647A142DDB6F2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js ....\../....."#.D&..*$..A....d.{v.^.G...d.W.:...P..k%..A..Eo.....A..Eo..... 8.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .q.-]../....."#.D..+$..A....d.{v.^.G...d.W.:...P..k%..A..Eo..... A..Eo.....y.j.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .J.L]../....."#.D...,$..A....d.{v.^.G...d.W.:...P..k%..A..Eo..... .....A..Eo.....a.....0\r..m.....M....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/plugin.js .;.j]../....."#.D...,$..A....d.{v.^.G...d.W.:...P..k%.. A..Eo.....A..Eo.....P.j.....

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):	696
Entropy (8bit):	5.628467661818252
Encrypted:	false
SSDEEP:	12:V9zo9PQy9z/a/j9PQzP9zC6i9PQU9zg9PQa:Xzo9PQuz/a/j9PQpzDi9PQkzg9PQ
MD5:	23A18D680C0A3E5A0AFBC06F122E9506
SHA1:	CB9E0EB558FF40A43AB4B96990A99413D0CCDE6D
SHA-256:	9863AF50DA5C4C142C556B727B5E1205C4C6077AB608305D8DE2EB3A695DCD46
SHA-512:	C3E52653B64647E3F3DF478EC61C9D423985CDFBF830A50BBEADEEADDDE373792571316064AE464384F9EE6A3ED08E25796ABDBDE9302B9F3954F4BE3B1902A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..<.\../....."#.D...)$..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....\.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js .P..]../....."#.Ds.A+$..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....d.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ..O<]../....."#.D...+$..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....+.....0\r..m.....,....._keyhttps://rna-resource.acrobat.com/init.js ...[]../....."#.DC.U,$..A.1.x.'.vI..*|Z..o...+.4....0..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	984

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0	
Entropy (8bit):	5.6279926184143045
Encrypted:	false
SSDEEP:	24:tB4v4KSBfB4v4/SBjB4v4QSB9B4v4TSB:nMVSBJMASBdMfSBXM8SB
MD5:	3BE53695CE234422ABEE7F4F53B5D8CB
SHA1:	7020B731CE0C9C7EC5743A10584493CC3E1C2985
SHA-256:	6499DF594BD11D1B26FDE03550677B1BE551676F2060D1C743D7245BCC88A1F4
SHA-512:	00F185A86F3C39186D1CE3E71C747108EDAF8172FEE259BC2C1259DFFC6E4ADA614A20B0DE67E6B8F50860979E41A7B266B4CF3A41697F4CF129883FD171DC1
Malicious:	false
Reputation:	low
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 ..j.\../....."#.DS..*$..A..hvDO.N.t@... ..n.*..... ....A..Eo.....A..Eo....._.C.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .3.,]../....."#.D..+$..A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....iV.....0\r..m.....v...n....._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js ...L]../....."#.D..,$..A..hvDO.N.t@.....n.*..... ....A..Eo.....A..Eo.....0\r..m.....v...n..... ._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/selector.js .|.i]../....."#.D..,$..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):	464
Entropy (8bit):	5.6824012215453115
Encrypted:	false
SSDEEP:	6:mNtVYOFLvEWdFCi5Rsth+ZiWulHyA1TK6tANtVYOFLvEWdFCi5RsONOgoZiWulHZ:lbRkiDQRWuss4bRkiD/NRWussbB
MD5:	F35C3A6DC889401C75D07F30989A91ED
SHA1:	E4C9C42F1EB964888893C0047F7F5ACCCD3600E5
SHA-256:	F19630FE4A844021BBF512871C45B8DB7C166104AFAC3D1E27EC13779AF66E8C
SHA-512:	649BDAB860431A96BD2617B0A6026A5911E2931F135358ADD7733DA263D01727D1A08598515A193CDEB98DCA57FB156D0B3FE0A4FDF0509FEF99B13065D7F56
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .A..\../....."#.D...*$..A..8 P..a...R..Y....7.@..2Dm{ ..A..Eo.....A..Eo.....Sn.....0\r..m.....h.....'....._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-tool-view.js .J.P]../....." #.D..%,$..A..8 P..a...R..Y....7.@..2Dm{..A..Eo.....A..Eo.....S.....

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):	420
Entropy (8bit):	5.541451190156464
Encrypted:	false
SSDEEP:	6:m+yiXYOFLvEWd7VIGXVuDAjuRVyh9PT41TK6tX+yiXYOFLvEWd7VIGXVu5zetRVg:pyixRulASV41TEUyixRuePV41TE8
MD5:	D230CB4D1E9D8B34C5CC996E9FBFBB5D
SHA1:	CD1A0BCA6003FC3CCE7FF4AEAD3501D74A2496A5
SHA-256:	42AA628DED160CB08045E42309B0AF79D3B5E3BBBD4AEF87E2DD275BD027327E
SHA-512:	02F29D19556D10946CE2D9BB76E37EFEB5792D75951EBA8BF059D2489BC472BF7F7585E1302C1BA72EDAE4BE3A819C2B915F7941D7884B4E50D7BD9172C4135 B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ..1-]../....."#.D...+$..Ak.Q.....-_..y.....O...>..1....A..Eo.....A..Eo. .....p.9a.....0\r..m.....R...kP]g...._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/selector.js ..j]../....."#.D..,$..Ak.Q.....-_..y.....O...>..1....A..Eo..... .....A..Eo.....x..i.....

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):	432
Entropy (8bit):	5.635546686361309
Encrypted:	false
SSDEEP:	6:mvYOFLvEWdhwjQouz4SLZIl6P41TK6tnMvYOFLvEWdhwjQpmi9LZIl6P41TK6tGt:0RhkYLZCFqRhkPi9LZC4t
MD5:	277244401EC67C5D109F91313B881D00
SHA1:	4FE78D138468F00479E4C924C8D340D7B265DE66
SHA-256:	04B64EB03BABFC71B954F67B5CCF79F1B4295E8B2A493A6797968567D35AA866
SHA-512:	2FF0E8ED8562EE7970C983F3C8AF3C514ED7F0EB93508304E62318D7A7F3DED1ECFB0A10660386241547F148CDA4BC45A69F166D67E9007A726E592CA261D50

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js .G.)]../....."#.D.I.+$..A.].>....uUf..N...k.....c..l.A..Eo.....A..Eo.....$..u.....0\r..m.....X.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/plugin.js ...f]../....."#.D@.,$..A.].>....uUf..N...k.....c..l.A..Eo.....A..Eo.....7.....

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):	418
Entropy (8bit):	5.540493450361182
Encrypted:	false
SSDEEP:	6:mJYOFLvEWdGQRQOdQd18tV6g1TK6tNlMJYOFLvEWdGQRQOdQpNVo2V6g1TK6t:2RHRQCptV1LGRHRQCEVo2V1
MD5:	A43355887A43C8A5C9B4AAD739078D58
SHA1:	9363D612FD813696E194DA469028BDBD3DC49118
SHA-256:	F250362F93AA4D0303F9DDDF9841C971FA0AA5E1B0230AF6DEA6342ECCABC15A
SHA-512:	55987EA74BEC77513A12BAD411F4A4C6E83538A6F16ECEAE240F7DFF9930464BD758F899FCF8FD5B49A08A576C21FD8296321FD912EC63FC4E642272D9F502C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js .g^-]../....."#.D{..+$..A..c..y/L....|y.n..C/l.....X7-ne.A..Eo.....A..Eo.....p.E.....0\r..m.....Q....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/plugin.js ...j]../....."#.Dj.,$..A..c..y/L....|y.n..C/l.....X7-ne.A..Eo.....A..Eo.....B.....

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):	716
Entropy (8bit):	5.625214312614962
Encrypted:	false
SSDEEP:	12:Z5MgOMuR/E75MGpgMuR/ExB5M62MuR/EE5M6+rUMuR/EO:ZSg/uR/E7SGpBuR/ExBSAuR/EESVrNuz
MD5:	CE4601E4C6F0B4C401317702B9EFCB37
SHA1:	89BB115476198619E1262AD0C54A4EDC617C70D6
SHA-256:	2D453497DCD5D9C588D89A096DD4F323FE20A5B664A23C36C6D0CFF0F5E29AE6
SHA-512:	7C3EFD2402C9B002E81C1E0531B8E50474D71659CBB9A2CEFBC2552C430A6FBAAC53FAC11E5B5D386BBBDA3CB05E0A9BB21AB4248F1D812FD8501D029F466 7D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..|.\../....."#.D...)$..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..%.]../....."#.DD.A+$..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ..U<]../....."#.D...+$..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....F.=.....0\r..m.....3....<lb...._keyhttps://rna-resource.acrobat.com/base_uris.js ...[]../....."#.D..U,$..A.y...L<?W.Xi..A\Q3...J.}...d..~G.A..Eo.....A..Eo.....*.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\39c14c1f4b086971_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.608049501159806
Encrypted:	false
SSDEEP:	6:mGpYOFLvEWdzAAu6SUe3wm0bbsIDMGH41TK6tby:XfRMkeKsIZE
MD5:	A8A41C5F227F3AF83F1F7D2ACA0494C3
SHA1:	1773D061F0D3E59F8F230004596291395A5330B4
SHA-256:	86AFD660857A099076BC452C5B46742F5AED55EA3C414B24E639EAED6EBDD415
SHA-512:	A7385CFCADCE46C940C4C77E1143AB63CC59F92228A1ACF2C943E9E5CB428A73FFB9015A7248F33AEC4A9CE0281EAD14F4670A7042B78260D758319F5A41E9 A
Malicious:	false
Reputation:	
Preview:	0\r..m.....T....,.^...._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/selector.js .7t5]../....."#.D..+$..A..`....^....L>..Xa./.....C.y.A..Eo.....A..Eo.....6.K.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\3a4ae3940784292a_0	
Category:	dropped
Size (bytes):	428
Entropy (8bit):	5.5365116835933845
Encrypted:	false
SSDEEP:	6:m4fPYOFLvEWdtuYMq9GM+by0zBUKSAA1TK6tQ84fPYOFLvEWdtu0BXuby0zBUKS9:pRnOM+beODRbwbeX
MD5:	0CB73DC32FBC276ADA89BE61295FE24E
SHA1:	4835A5618F324F07A7E1543F14C013DB99A0D9ED
SHA-256:	B0386C1D325DACA873142CB92B8774EE239B656F1C263C17026744551C8F0EC7
SHA-512:	AF2533BB4712B971EC059DA3017B5C0B7EABF2000FAB7472FCDC60228AC3750C6C3B91C881FAF4174651EB075C83B8F6E81A73C0FA71CD49212DC612B415323
Malicious:	false
Preview:	0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ....]../....."#.D..+$..AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....ti.....0\r..m.....V....._keyhttps://rna-resource.acrobat.com/static/js/plugins/search-summary/js/selector.js ...k]../....."#.D.~.,$..AQ..E.=....=h`t..t..3%A.F$..w..A..Eo.....A..Eo.....|.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	708
Entropy (8bit):	5.601003014158166
Encrypted:	false
SSDEEP:	12:KkXxKMSCvgYtUlSfakXxKMSCvBQ1tUlRkXxKMSCvg/tUlPkXxKMSCvHB08ItUlw:KkXxiC4YWSfakXxiCpMWRkXxiC0WPkXU
MD5:	A2B1035DCC2C9EEE93C18F57B552EA3F
SHA1:	36F371943EF80B5AFDD17CE17F0D11644A0749AC
SHA-256:	CEE73F5F3625A1A9B290AADBA22992B480086F3FBCA31BB4FF9B4BD33DA91FEB
SHA-512:	29C40DF9EF64A6C260C579394CF9398E558541B917CB1AF58D5D2B610B812F058E53DC3835C20A2C39E006BF653F210EFAA305239BEE653998D8C334CD546BF
Malicious:	false
Preview:	0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..z.\../....."#.D..)$..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....Qq.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .;..]../....."#.D..A+$..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....s~L.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js ..S<]../....."#.D...+$..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....M.....0\r..m.....1.....5...._keyhttps://rna-resource.acrobat.com/plugins.js .p.[]../....."#.D..U,$..A.PU ....t^.....a.k..u.7.M.BW6#}..A..Eo.....A..Eo.....C/@.....

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):	748
Entropy (8bit):	5.6062846242219555
Encrypted:	false
SSDEEP:	12:5h6OLU910PPfkgh6OLg/OPfkTllbh6OL36Pfk2h6OL6/YPfkb:5h6xXq8gh6xg8Tllbh6Ik82h6G8b
MD5:	57403A3B528F5C51CCE382E8D8B5C57E
SHA1:	FA4CC8B74FD287FAF028069F5A184797E972E449
SHA-256:	E62F3CA7C1EE94EF59342FB151192DD4D915CDE4DDEC3CE7CE526C075B0A0F8A
SHA-512:	CEBCDCE1980848F7FA074FE41189C9E6B11737B1C275DCDD477296AD7F8F56CA8D8167218E5B558D475F0470FA05B403A6EF135F21E8BD0B84909735D7E5EDE D
Malicious:	false
Preview:	0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ....\../....."#.D/..)$..A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...&]../....."#.D0.s+$..A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....X.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js .:II]../....."#.DjP.,$..A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....S.....0\r..m.....;...I....._keyhttps://rna-resource.acrobat.com/static/js/desktop.js ...d]../....."#.D.[y,$..A..q.O...j...._y..L^z...?..@N..A..Eo.....A..Eo.....m..B.....

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):	976
Entropy (8bit):	5.662835999402258
Encrypted:	false
SSDEEP:	24:UB4v4ktXwzXLn+8B4v4iwzXLnhB4v4UGwzXLn9kB4v4vwzXLn:8MEbn+0Mqbn7Mlzbn9sMNbn
MD5:	7BAE80536A7AAE218BEF06282F09B1BF
SHA1:	2246D4F81C9C383C81620DA759E43C59B36E1452
SHA-256:	0B3C4A00936105B15F9E12DAF108E2C2B846B1483374338E3F9F8BF153128F58
SHA-512:	271829FB2B26751B6ADBCAAC98563E525519E949D37C34CDEB2EFA4934A1645A58B4279876645F6C8A303B527A808645EF0C792F94F9762835CE569F3E70B0A7
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0	
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 ....\../....."#.D.Z.*$..A.....H...{...2. ./.k`..r4.C. .A..Eo.....A..Eo.....J.:w.....0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js .T7-]../....."#.DK.+$..A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....x.....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 .ZYM]../....."#.D.J.,$..A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....^@!e.....0\r..m.....t...R.1<...._keyhttps://rna-resource.acrobat.com/static/js/plugins/tracked-send/js/plugins/tracked-send/js/home-view/plugin.js ...j]../....."#.D.:.,$..A.....H...{...2../.k`..r4.C. .A..Eo.....A..Eo.....C*.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6267ed4d4a13f54b_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.568327051634295
Encrypted:	false
SSDEEP:	6:mq9YOFLvEWdzAHdQnw2t5GFCaa+41TK6t:NRMHdkt5Gda+E
MD5:	8128A5C1996880AFC0A1E559FEC325E2
SHA1:	693E2491DFB3D715B7A8B467AD7579EEFB73D069
SHA-256:	E7815C18B28E2020BBBF382E8887583094ED140A6EC5329DC2BD45E474E52E66
SHA-512:	68BDC54A74F71C1A4D1CAA682B0FF727BBF0459B51EB9C7752048427F2081784818ECBA6CC4D2C5EDB1A9D300765ABC7B643073CF1304E72C296CA62AFAF92C
Malicious:	false
Preview:	0\r..m.....R....L....._keyhttps://rna-resource.acrobat.com/static/js/plugins/walk-through/js/plugin.js .8.5]../....."#.D/..+$..A...G.3D.....Q.g0...._.Q.....A..Eo.....A..Eo.....&.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	422
Entropy (8bit):	5.50450354104815
Encrypted:	false
SSDEEP:	6:ms2VYOFLvEWdvBIEGdeXu3nIKP11TK6tY8s2VYOFLvEWdvBIEGdeXuW4AkBw511o:BsR2Ese0nN0sR2EsexmwX
MD5:	96CE68FA715C58048F1B3A7696443077
SHA1:	B3A3D4B518714CE5DE799F39988927864D1DB32B
SHA-256:	02C57693AABE956B241803325B2E3B8C7ACC3A741D979F780430652D3695C514
SHA-512:	65AFBD83DDF6CF4A37DF23BCB3DEA20372DA0C8CC08798F72372120A10AF19D7DC945B0B3FAFFC53E64F479A62C421CB55ED78C2CAFFD13E113BC8748C4FD9E
Malicious:	false
Preview:	0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .8L,]../....."#.D.<.+$..A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo.....` .....0\r..m.....S...]....._keyhttps://rna-resource.acrobat.com/static/js/plugins/add-account/js/selector.js .i.i]../....."#.D.;.,$..A.A.o]@r..Q.....<w.....].n\....A..Eo.....A..Eo....._.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.676464921340082
Encrypted:	false
SSDEEP:	6:maVYOFLvEWdwAPCQZQuo3B7OhKlvA1TK6twaVYOFLvEWdwAPCQyk8TB7OhKlvA13:RbR16rn3BJkFbR16Nk8TBJk
MD5:	8182010E9D435C1FC61BC9EF39EEF6B2
SHA1:	6A9A64B02AE88D341DD8D161E64CD1C7790F6307
SHA-256:	AB2CD41A94DB48049290F8408CB85B8521893C9F356E9D415C30F960830F5BE3
SHA-512:	F1497BFCEEE4DA61F58B9A153D408893C557A956FAFAF2FA9AEFDC3B8071D94A8C8C432BEFE3E78A915561AC450E5344370F33A4BACD85ECB3E334D1B5709E18
Malicious:	false
Preview:	0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js .2()../....."#.D^,.+$..A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....~..... 0\r..m.....J.....{...._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/plugin.js ...f]../....."#.Dl..,$..A..4T].....Tw.....(..b...EO....9.A..Eo.....A..Eo.....!&.t.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	422
Entropy (8bit):	5.592713893830594

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0	
Encrypted:	false
SSDEEP:	6:ms2gEYOFLvEWdGQRQVuCKyUy9BnQdFt1TK6tJs2gEYOFLvEWdGQRQVuuRQLQdFt5:B2geRHRQhbL042geRHRQ7Rg0
MD5:	FE4E26BAB97227E0557A050A5EEAC208
SHA1:	7D80FA2C88FE5985EF92BA88DF6500D938BEFF27
SHA-256:	B14EAF498FE89AB1868EF75494F9914B05919676834C9CE85ADA49F00B53F31F
SHA-512:	76A2C1A7204E453B4A90AC16AD73973B855A2CA07DE33A11A2F3DB04B30AA7B4B95A04CF1D2C566C2D6D13D1E67B1C5B9AE985E896C826856CDC478571EEB7 6D
Malicious:	false
Preview:	0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js ...,]../....."#.D.1.+$..A@..{o]...9o|..qY....T....{..u.b..A..Eo.....A. .Eo.....^.....0\r..m.....S...W.%z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-computer/js/selector.js .5.i]../....."#.D...,$..A@..{o]...9o|..qY....T....{..u.b..A..Eo .....A..Eo.....)L.....

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):	824
Entropy (8bit):	5.667470723435364
Encrypted:	false
SSDEEP:	12:WyeRlFQEt1w60yeRliN1Et1w3MyeRlXlAVt1weMyeRlGt1wA:WJLfw60JaN1Efw3MJvlOfweMJufw
MD5:	F9C8198A3FDE6F5843A5E67A608760BD
SHA1:	ECB81580A0B2E7D2799D4CB9E746D95B1D6F9681
SHA-256:	97FDDDB2E8D3B1991DC6AAE660231FEF66C833DC07DFBE811767ED938A8107D9
SHA-512:	B16EC836078D56B173EDE202E7CFB257A4D31A082AC776C98C0FC7B93370B9081E4D5B67A481ACA09608477CD7C1671639B26D077FE852862E1504BD4819E10I
Malicious:	false
Preview:	0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js .F..\../....."#.DR..)$..A.t\a.....x5.'OuE.C..@.....x..A..Eo.....A..Eo.... ..GF.%.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..a']../....."#.D.2{+$..A.t\a.....x5.'OuE.C..@.....x..A..Eo..... .....A..Eo.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..lJ]../....."#.D...,$..A.t\a.....x5.'OuE.C..@.....x..A..Eo..... .....A..Eo.....I.....0\r..m.....N..../....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/plugin.js ..e]../....."#.D.-},$..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):	436
Entropy (8bit):	5.580180738491977
Encrypted:	false
SSDEEP:	6:mnYOFLvEWdhwyu8kfWsqwK+41TK6tkt2nYOFLvEWdhwyuXPnqwK+41TK6t:wRhsfW9wK+EytgRhwqwK+E
MD5:	82D75CC2EE204331406B8269A1FDCF79
SHA1:	7E892BF0AF135ECDE30BEB68BEE5E24E7DF86A1B
SHA-256:	C6529605EA1B9B9B7B226BCF7C9AA0F27CD8E0D6A46F2556C9268A8E24D4A5B1
SHA-512:	CD627761FAE3D2868DE3AE606FF7B122A002A5B07E238724A9FBA56924DF860308FD5172F0672B090C3B9F4DA6D464CFE22161D6F01BDED0B8DA46FC21128E5
Malicious:	false
Preview:	0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js ...)]../....."#.D4.+$..A.....7...o..a=.98I.....(3.$G.A..Eo..... ..A..Eo.....N.....0\r..m.....Z....._keyhttps://rna-resource.acrobat.com/static/js/plugins/sign-services-auth/js/selector.js .h.f]../....."#.D{i.,$..A.....7...o..a=.98I.....(3. $G.A..Eo.....A..Eo.....U..j.....

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):	920
Entropy (8bit):	5.63725187510299
Encrypted:	false
SSDEEP:	12:/RrROk/LfLE3RrROk/UBCfLE/RrROk/fmlEfLEQRrROk/HCfLE:/PJ/L43PJ/Ug4/PJ/fSE4QPJ/HC4
MD5:	914136F498D932A01EF0B6D1DD5C977E
SHA1:	3B7053AFD90B27AAC9ACBF8858F13DF321A037A1
SHA-256:	6F9E2FF3F8A4E27853C453AEE42724D0D1AB095742164EF9512744F22B327E75
SHA-512:	0969AC2ABA91D9920F3AB00665D69A440E1C8CC1B380887D9919266CC54F21C858097A07453857921F7C9EB4DAC86B29D0DCE0A454B77BA05FC820DD3408312
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0	
Preview:	0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..g.\../....."#.D'..)$..A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....U|.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .._']../....."#.Ds.{+$..A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....zWy.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js .jJ]../....."#.D..,$..A..~..rw.+[....!.)?..f.U..(=.=.A..Eo.....A..Eo.....B,.....0\r..m.....f...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/selector.js ..Ze]../....."#.D*.},$..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):	744
Entropy (8bit):	5.6194984270444515
Encrypted:	false
SSDEEP:	12:xqT7ECPLnjqTJ4CPLnsBqTL4/vCPLnEqTYBwCPLnQD:A0MnmF4MnsQQMn7DMnQ
MD5:	8208BB103E69FD920A1B3FFEAA87B445
SHA1:	42F73A4378AF20635348E44F060B3FBEFD1ABF67
SHA-256:	5EFB9BC037BE67C77594C0B274A32F87F967A3A60788ECDA1D262DE3C62E1A15
SHA-512:	B571A10021270A521456BDB3BF0604DAC2D35450C0E6FBDD2305344384915C54A3E588BF75C3E57CD2FCA51A76A705595A7E6E364841CE7B7A3FBF77BA59F10
Malicious:	false
Preview:	0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ....\../....."#.D...)$..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....m.%.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...&]../....."#.D..r+$..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....x.c.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js .#WI]../....."#.D...,$..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....G.....0\r..m.....:....f....._keyhttps://rna-resource.acrobat.com/static/js/config.js ...d]../....."#.DDQy,$..A..~]...%s..<...n.f..<.....1#..U..A..Eo.....A..Eo.....H.V.....

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):	828
Entropy (8bit):	5.622272417670471
Encrypted:	false
SSDEEP:	12:zRMBxH/sD0ZRMtpVsD1RMuj4IsDFBRMTbIsDm:zYxHUD0Z7D1q7DbQb7Dm
MD5:	8B6B742D0E86216101189F4548C5D95D
SHA1:	1F4BDF6C5A14D13FEE9DD2E3150AC276333F21A3
SHA-256:	DFBDA1C956E88466525F50492C046F6D1E0259E4291CC0A8C2BCA6CD20892CED
SHA-512:	1CFCB32DB2731995EFB2DC05D420C1ABB5A35BFA99B42512DB29E0A1319A03140B5955DF473F3C34FCC1D49A735F118BE46A5E1045661243FA1FDE40923F403
Malicious:	false
Preview:	0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..b.\../....."#.D.n.*$..A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....=.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js ..r,]../....."#.Dvo.+$..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 ..zL]../....."#.D...,$..A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....#.....0\r..m.....O...a.Y....._keyhttps://rna-resource.acrobat.com/static/js/plugins/reviews/js/selector.js .P.j]../....."#.D.m.,$..A..z._a...'.v.....4p3..1.']...A..Eo.....A..Eo.....3-.b.....

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):	840
Entropy (8bit):	5.562869789736162
Encrypted:	false
SSDEEP:	12:6lJRf1SFoMmuclJRWSFoMzlJRwoiMSFoMvzlJRe2hSFoMz:YB1SFoMmpwSFoMHyKSFoMvHhhSFoMz
MD5:	EA8614B06A9D90B0D58EA90EB00CAF7B
SHA1:	FA29C8D049B991F23D8DA52D01A9F81621536964
SHA-256:	7C3CA1710FB1C9A12ADA9ED1CC49077654A6FB1686EB9339062E471278257756
SHA-512:	7B97DF712E65AB8917CBBF6BD6FD172C08B84F345987F53C2D16FC029B993A908E8964BDF542999AB1DBC9EAF3741051119DEECF8118C78F96571A2CFD26CA0C
Malicious:	false
Preview:	0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..g.\../....."#.D..*$..Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....A.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js .ut,]../....."#.D..+$..Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo.....].n.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..{L]../....."#.D0..,$..Ac}.H7M=M..-.....Ix..R.l..}Rl.$q.A..Eo.....A..Eo.....3.31.....0\r..m.....R....|...._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/selector.js ..j]../....."#.DI..,$..Ac}.H7M=M..-.....Ix..R.l...}Rl.$q.A..Eo.....A..Eo...../..A.....

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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0	
Category:	dropped
Size (bytes):	892
Entropy (8bit):	5.626685598881936
Encrypted:	false
SSDEEP:	12:F8hRrROk/15ak+e2QU8hRrROk/IkHe2sv8hRrROk/sBve2F8hRrROk/Z3Ve2:UPJ/vt2QVPJ/k2rPJ/sBm2UPJ/Z3Q2
MD5:	5F4B82EBD56FE282FF8F13538D0342B5
SHA1:	96C55955DD2AE0C02900208F06E67D3116C38B63
SHA-256:	88E08BBE3E09BF5552DD4B04DB45E8C6D6662E7EE0ADB6942C7E43D8A72891C8
SHA-512:	10C78411DB20FDDB6F9E7F28DB1D5074F299F97737A6F1486B430CEE6B00598439CD70198F4268F292E0743CED1FB859CDAAA2111352523E8CAD6F4702B5B990
Malicious:	false
Preview:	0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..c.\../....."#.DK..)$..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....;.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ...']../....."#.D..z+$..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 ..lJ]../....."#.DNb.,$..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo....."D.=.....0\r..m....._...h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/selector.js ..Oe]../....."#.Du.},$..A..%.k.SZ..~W.....:)'B..ad.....A..Eo.....A..Eo.....K.....

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):	852
Entropy (8bit):	5.69266123226785
Encrypted:	false
SSDEEP:	24:ehQ3JICOhFne+JICEmhGHHJICphFOJICR:eqVOrn5EmWp/y
MD5:	A76996EA44AEF2C502FC4EC4B3ABDB00
SHA1:	6D0EFB415DC149FCB84743A95DE7F4F0510E4783
SHA-256:	08065827FD397C8DE77074CEAE7E7DF6B41C5AF7177B073DA40ED16ACD487414
SHA-512:	F007679577CE96EA53A6041ED732271A99B314B3CB97DB0B09A2B8A08CB34ADD19DCFDBE488A7F4A3B9D9B72A5A641765D334669805231DCD920AF19D5C28E F
Malicious:	false
Preview:	0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ....\../....."#.D...)$..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..c']../....."#.Dz.{+$..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....1..u.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js ..oJ]../....."#.D...,$..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....P.e.....0\r..m.....U....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files-select/js/plugin.js .=.e]../....."#.D.X},$..A.;"./N_.,.:C..2....9L.H...3:...A..Eo.....A..Eo.....d.....

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):	832
Entropy (8bit):	5.600414062936033
Encrypted:	false
SSDEEP:	6:mOEYOFLvEWdrIhuewQAeG/bLzgm2d/1TK6tY/2OEYOFLvEWdrIhuYS9Lzgm2d/1Z:0RhQAH3ReOkRtRevCRdORe5Rv3Red
MD5:	3EE9BD63B10B03EB327C5BAD7985B2E3
SHA1:	0B1F5F700182097896E48637AD48446A893EF2F3
SHA-256:	65E62230838D6D9E2B48D197E3434C05DC932709D2B83DAEF1DD41699F0247CA
SHA-512:	27A2C200BFD1D88C63689E4388E34E95973F724CD136B082A11719361FF0F7EAE343EC97C4C13EDE09BFB9C970715D2E311C207534A1E1BD9C841DCB9E1040F
Malicious:	false
Preview:	0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ./>.\../....."#.D.u.)$..AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..*']../....."#.D.qz+$..AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..GJ]../....."#.Dy..,$..AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....s.....0\r..m.....P....r....._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-files/js/selector.js ..7e]../....."#.D..|,$..AZ.Z}Q..4.o....0+..[|..n:*..U.W.A..Eo.....A..Eo.....9.....

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):	752
Entropy (8bit):	5.648931326539139
Encrypted:	false
SSDEEP:	6:mAElVYOFLvEW1KY2kx56uvp1TK6tveAElVYOFLvEW1KV8azoI2kx56uvp1TK6tH6:6JJKY9sJJKV8az3heJJK0bYJJKFwop
MD5:	56299721DD4C6530F843B99B3BE2351B
SHA1:	18A929B53F8A64276C08EE81EBB0A121C641CB97
SHA-256:	8F836A3C6FA1DC7FCAEF6F3FC78728F8E66467B926057DCA3F883BB0057B78C4

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0	
SHA-512:	19E8C9A1A3399EB254181880A0D0EDA963099612D6752A1E25601263569580FC7DECB66B38120426BEB6CBF4175AF3CCBA34811E056D769B3B932D03CA996E5F
Malicious:	false
Preview:	0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ....\../....."#.D...)$..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....!.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .uB.]../....."#.DY.S+$..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....~.....0\r..m.....<...)6....._keyhttps://rna-resource.acrobat.com/static/js/rna-main.js ...?]../....."#.D...+$..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....i.";.....0\r..m.....<...)6.....keyhttps://rna-resource.acrobat.com/static/js/rna-main.js .}.]]../....."#.D..e,$..Az?...SwC...^..y.....V..7R-O.....A..Eo.....A..Eo.....j.....

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):	428
Entropy (8bit):	5.663310150619116
Encrypted:	false
SSDEEP:	6:mWYOFLvEWdBJvvuVr9V9ghUDLYtmOZn1TK6tQ2WYOFLvEWdBJvvuSZkA7ihUDLY7:xRBJ8RdDcFZL8RBJrkkDcFZL5
MD5:	D46F75CA933ADA4C997ACDA3FFAEEB79
SHA1:	01F747A4FA69FD3B16CBD0C7831DB0AAA547E9EA
SHA-256:	205F2303B3F397CB43407CE9BF08880915ADFDA9689EE0C88151D9AFF05328F6
SHA-512:	B599C9B7FD35DB3734BD4DDE1B688CFDD75C365E100C84E20FC2AF096A717AD50FA4530403887BF3A8A3E071C9F36CD3CCB1A4FBACC69C14971F621DB560162
Malicious:	false
Preview:	0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js ..O,]../....."#.D.S.+$..A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....0\r..m.....V.....h....._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/selector.js .O.i]../....."#.D.P.,$..A....t.q..W.EZ....1...[.zC.7mD..A..Eo.....A..Eo.....!{.>.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	844
Entropy (8bit):	5.653999525607323
Encrypted:	false
SSDEEP:	12:BPHlHPcd5PHCEHc29rPHfGcol7PHwctl:BPHRPcd5PHCEHc25PHecol7PHwcX
MD5:	11018FECACFB72042B06F0CE924D7BE2
SHA1:	CFD84F7133C0F2DF4B02BEBA143BFE101C754EE9
SHA-256:	1FACE49C784B38E5B21B0AB64F9A780D74112C5694FFA3A10C16EE83DD8B1D33
SHA-512:	EFB3F433024370CC6895D74B474F10143AFD45887435BA1BE34109A9DEC6FFE5268150DBE1F888EDABD34876C5E46C2626DCB7229E464E5C5A498B2B54C87B2
Malicious:	false
Preview:	0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js .4~.\../....."#.D.t.)$..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....N%.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..'.]../....."#.DM.A+$..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....2.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ..`<]../....."#.D+2.+$..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....@W.{.....0\r..m.....S...{.j....._keyhttps://rna-resource.acrobat.com/static/js/libs/require/2.1.15/require.min.js ...[]../....."#.DlBU,$..A...L...Im.@.....E.nW...IP..A..Eo.....A..Eo.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf0ac66ae1eb4a7f_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.637396682855327
Encrypted:	false
SSDEEP:	6:mKPYOFLvEWdENU9QIYhdiM3Y1TK6thKPYOFLvEWdENU9Q/krS9iM3Y1TK6t:bJRT9Ar0KJRT97rS9r0
MD5:	2A79BD91B1EDC6D817909306557F2742
SHA1:	937BC140B55D365F6AD903D7A62DF4A2E5EA2E9B
SHA-256:	A6972949F052410103224557C329B1C7C41E034EF63FA41FA534460666DF72B3
SHA-512:	FAD87E3B886C0332B1DF088496F575921C84202876C2A1F5212108571A0C820A023E77F5A088C5AEA83A37ACCC50D773A5BE0268082DCF1DACF294489D81AB6
Malicious:	false
Preview:	0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .qr)]../....."#.D..+$..A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....0\r..m.....P...Yft....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/plugin.js .@.f]../....."#.D...,$..A...M....m+lS..e.....<7.U.P8*.0K.A..Eo.....A..Eo.....|x.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0	
Size (bytes):	416
Entropy (8bit):	5.6188616704636205
Encrypted:	false
SSDEEP:	6:mQt6EYOFLvEWdccAHQzhjBRCh/41TK6tI2Qt6EYOFLvEWdccAHQGJB9hjBRCh/4v:XRc9OhDi/E2Rc9rDi/E
MD5:	3B0676D606E47DA344E6AFE3D16646B1
SHA1:	4D6915C0EAA947FABA7ED6EC3E96DF7A0C577E6D
SHA-256:	8FCC0F734F0BA2B2B8B05F05A8F560B30532C6ABF6EFEA13ADC88DBDB5AF81E3
SHA-512:	E48ECC65AE91BD56476DCCD2D4A4DF4337AD8A40B02A42AEFAB48E21FB15639631BEE155D690DD59F89A7A3CBE1A005E10EE35738B0BFE29BEE8A2F2A305135A
Malicious:	false
Preview:	0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ..:-]../....."#.D_..+$..APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....0\r..m.....P...W3....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/plugin.js ...j]../....."#.D...,$..APJm...0x.x..RD...BB!@5..<..]....A..Eo.....A..Eo.....\.U.....

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):	462
Entropy (8bit):	5.618863272865798
Encrypted:	false
SSDEEP:	6:mqs6XYOFLvEWdFCi5mhuq5zULlF4r1TK6t+qs6XYOFLvEWdFCi5mhuLbsULlF4rP:bs6xRki0eLlF4n5s6xRkitLlF4nr
MD5:	EDDEAEDA2C2CFC10BC647A97B8F27D39
SHA1:	C40A6A64FB3250BF2133B1DCD3EE1382530552CE
SHA-256:	40220942CC1ED923A72F4AE99AB89A1944F661E65FA57D009F60DC018907294F
SHA-512:	13024231E4A612E60354A3E654687403873D9AAD263FAC1157ABA3B87AD2DA63E4DF994D055FBE5A47A8A553DDB16DF9E4C9992BF3F8E0590CB53B210259FEDF
Malicious:	false
Preview:	0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ....\../....."#.D1@.)$..A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....4.....0\r..m.....g...~.I?...._keyhttps://rna-resource.acrobat.com/static/js/plugins/aicuc/js/plugins/rhp/exportpdf-rna-selector.js ...K]../....."#.DFy.,$..A.P...#4..l....5...5..).w.. .h.~..A..Eo.....A..Eo.....,i.....

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):	430
Entropy (8bit):	5.526501558724536
Encrypted:	false
SSDEEP:	6:mhYOFLvEWd/aFuzHGw941TK6t4UNMhYOFLvEWd/aFuvgzL1941TK6tN6F:WR5HGw9EGkYRBA9EaF
MD5:	67E7DC8A71FF93A6786955E9ADAF14E3
SHA1:	DF5E4D7BDE07A6DD094275DC1558C198E51696B7
SHA-256:	833565B6A1CF90F9915DFF93BD691F86FE63E0C0D5FC65931C22CA3E8B02E64D
SHA-512:	5CA114732EFB0237BF32F31975AC022BEE9CAA8DC4B68ED41F3C1F2F8C5E338418A5BE630924D86F2D27D0636D965D77CE6AD848D77ED301EEE341F6607ACB1
Malicious:	false
Preview:	0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js ..(.]../....."#.D...+$..A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo.....0\r..m.....W....w.m...._keyhttps://rna-resource.acrobat.com/static/js/plugins/my-recent-files/js/selector.js . .k]../....."#.D..,$..A...a.f.m.i.o.p..3U5.....^...I.A..Eo.....A..Eo....._.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.538517578496209
Encrypted:	false
SSDEEP:	6:mR9YOFLvEWd7VIGXOdQDt9k52oBMqVd3G4K41TK6t0R9YOFLvEWd7VIGXOdQ7Xow:2DRuR8PyB9Vd2kaDRuRcYB9Vd2kkF/
MD5:	038BE1EE36F694CA8F0F921FDC19E40A
SHA1:	580B5EAA999D182E86E5F1613BA5D3E7F21A5C5F
SHA-256:	869FC073EFDCD42A996A5E437625AE8B95AB0DF460545D638635202433325FBE
SHA-512:	BC81E643F922ECBEB0324B1B1E80F17698E57943536662FBD894E2B63602FE13959C2F738DDE22CCD52EDFAF9C9375454E3F9711462165885E55EB8EDE494F71
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\de789e80edd740d6_0	
Preview:	0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js ...-]../....."#.Dj.+$..A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....0\r..m.....P...y.p....._keyhttps://rna-resource.acrobat.com/static/js/plugins/app-center/js/plugin.js .&Jk]../....."#.D...,$..A..y.$..$.v5j...T...z.]..._S....A..Eo.....A..Eo.....uS.....

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):	832
Entropy (8bit):	5.635579484262546
Encrypted:	false
SSDEEP:	12:+RQG5Grnm2RQWmcrnYORQGi2rn8X8RQYVZYhrnx:+v5qnP9nYOC6n8sRLCnx
MD5:	7B2EFF7923133002F94A3185C2A5DD9F
SHA1:	09AC70227452C9E243519A0593B9ABC603C9426D
SHA-256:	9B3174824F42D3F6F45D3C24F96BCD6C1E6564717B54FF3E44964FA6A8658D9E
SHA-512:	BF211A4C382FD30A94FB356F1C38F09F8535C5533D95839855CEB458304EF2E5ADCF8BB9951D39E66AADE33CA2B49A6B82075FC38FA691CAB909B3A3231D4D1 3
Malicious:	false
Preview:	0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ....\../....."#.Dc..*$..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....4\.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ...-]../....."#.D...+$..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 .mXM]../....."#.Dzo.,$..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....5.;.....0\r..m.....P...gT....._keyhttps://rna-resource.acrobat.com/static/js/plugins/signatures/js/plugin.js ..8k]../....."#.D...,$..A#..@..k(v.8g..5.~_....]Pj.*..6.A..Eo.....A..Eo.....f.....

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):	420
Entropy (8bit):	5.600848132184165
Encrypted:	false
SSDEEP:	6:moXXYOFLvEWdENUAuu4APuyC8n1TK6tuEoXXYOFLvEWdENUAu5MyC8n1TK6t:xhRTo1u7QKhRTc7Q
MD5:	4E41E2A64F6FCB4B41EB2045795A6221
SHA1:	F5C91480D2969093CF29C61A52F857BDE58652AD
SHA-256:	6BBE08D3FB8F7C6DF09842B9F17340FB678451BE1FD54FB52CFE884B76749DEA
SHA-512:	731A8572C4F0BC4637D3FAD7BA4412DE0D1601E52E74C4494D9FBB1CF48009B1038D4FAFF50255A1FFB927DA9676D8B84E70577C98AD56F2AD223EC68013EA2 A
Malicious:	false
Preview:	0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .M.)]../....."#.DD.+$..A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....f.....0\r..m.....R....._keyhttps://rna-resource.acrobat.com/static/js/plugins/uss-search/js/selector.js .).f]../....."#.D*V.,$..A8.../...;.\\o....1.....+..A..Eo.....A..Eo.....|.....

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe
File Type:	data
Category:	dropped
Size (bytes):	884
Entropy (8bit):	5.6363541128347645
Encrypted:	false
SSDEEP:	12:nRrROk/V8KNmmRrROk/VCPm1RrROk/Vibldm8fRrROk/Vum:nPJ/qBmPJ/0O1PJ/obloUPJ/F
MD5:	A792F7E9F937296CEAC479E853B98327
SHA1:	27C52E4DD311C18CA070229B32D8CA81E0919502
SHA-256:	87EE82F5FC23041B07BC15B3087AA5AE670651C2A7AD620538FD6D5F0F118081
SHA-512:	B72D3065CDA7B4C16FCB6B6CE7ACE5ABF918EE13AE87F6BA9BD807D5B15E8D8568B0B67B898E82608D7128CC24ED11512184102C431D25E706C6A72EBCE6A 12
Malicious:	false
Preview:	0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .V..\../....."#.D-..)$..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....I.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .S.']../....."#.D].{+$..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .%.J]../....."#.D-C.,$..A ./.ev.....N~..6.b.....$.j;:C...A..Eo.....A..Eo.....0\r..m.....]....,...._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files/js/plugin.js .v.e]../....."#.Dbf},$..A ./.ev.....N~..6.b.....$.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

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0	
Size (bytes):	420
Entropy (8bit):	5.600724766705491
Encrypted:	false
SSDEEP:	6:mZ/lXYOFLvEWdccAWuC4/wnxAdm9741TK6taHeZ/lXYOFLvEWdccAWufiAdm974M:qxRcw46Adu7E8HSxRcUAdu7E
MD5:	A87DD7D96F6E3C88F393715F7D5020FA
SHA1:	D74F7F27DF39A869C767BBC744B6667BBCD5182B
SHA-256:	609F742E6FFD13D4DE98D962D394E9102A6175CF8366379C4CFB9F742F7D3076
SHA-512:	F5738E95D0449C56D55D101923E881B455C41A6D38E357790AAA7977EAA36E8C42B51AB2A5DAEA0D643F119BF29F1C29043A140BF09994E0C1833EE8BF3F8325
Malicious:	false
Preview:	0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .#.,]../....."#.D.!.+$..A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....m.....0\r..m.....R...F....._keyhttps://rna-resource.acrobat.com/static/js/plugins/scan-files/js/selector.js .T.i]../....."#.D@..,$..A...U...I.>P...X...x..0U.~;m.x.k.A..Eo.....A..Eo.....+.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):	408
Entropy (8bit):	5.623103082193041
Encrypted:	false
SSDEEP:	6:mMOYOFLvEWdwAPVuirK/KeESkJn1TK6tJMOYOFLvEWdwAPVuhtbzJn1TK6t:2R11FeeLbR1oFL
MD5:	99A9BF6ABF11D0A1EB50EF4799FEB222
SHA1:	EB4D263D26D3D40DB583093D9847DAC4136BC684
SHA-256:	E28A25ADAFCFDF32A251900191B7454AF1E11DAE6B9E696E622EBB22AD428464
SHA-512:	8264F22FFA2A70575700112EF71B92290864154640A5C437E5C1159679DF41473B23602E4A3F97BC7ECB0193496218A29FBA29632BB640B54FAEB7E82CA56062
Malicious:	false
Preview:	0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js .v.)]../....."#.DU..+$..A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....'.....0\r..m.....L....Ey....._keyhttps://rna-resource.acrobat.com/static/js/plugins/home/js/selector.js ...f]../....."#.D.7.,$..A.....k....F..D..O.n;[.1m.....=..A..Eo.....A..Eo.....+6W.....

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):	424
Entropy (8bit):	5.617038931872953
Encrypted:	false
SSDEEP:	6:m3PXYOFLvEWdBJvYQaNQzhcsBXIh1TK6t13PXYOFLvEWdBJvYQ/j4XzhcsBXIh1g:mxRBJQiDB0bxRBJQhDB02
MD5:	C36875E5AD10C89365D5B8889181D159
SHA1:	624863DB109162A175DD527EA21D3300AA130061
SHA-256:	704CE115988544E877B7959BF7E9486DCF20190DC36F8C84FA26AD71B85278FC
SHA-512:	6B8AB01F0BDE73BD0F51A6F4122DE0F41F66C1639ADCB220D5C2A657858CBBF46648ECB99D578B7C056D5A69E6DBF60CF73C93CE9C774D2CA55532AF6152D 57
Malicious:	false
Preview:	0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js .T`-]../....."#.D...+$..A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....lV.....0\r..m.....T.....z...._keyhttps://rna-resource.acrobat.com/static/js/plugins/activity-badge/js/plugin.js ...j]../....."#.D...,$..A...k..`..N3.... ..d..$[.....{.A..Eo.....A..Eo.....e.....

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:	modified
Size (bytes):	912
Entropy (8bit):	5.6541633753695075
Encrypted:	false
SSDEEP:	12:3RrROk/s3tcFRrROk/sZMcYHRrROk/sKSc2chVRrROk/sEc:3PJ/RFPJ/WJAPJ/JSc/LPJ/K
MD5:	060B9D9F5E799D688C8A67B2295A2267
SHA1:	6C2D29A1339ED6B683A600F48D3555FE42746E91
SHA-256:	B8A6639C9E986910BC52E92DD2CB4E1540F61B879CE15E5D3FD73648E1CEE4F6
SHA-512:	FEDCAB9CCB14CBB267736554F3A51E90A70246C40D47DADFF7836E240CCC4FBCF47974550B887C80B5B68DDC85B1481EAF3F6F9654AA330364E8B11279D7A4 0
Malicious:	false

C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0	
Preview:	0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .R..\../....."#.D...)$..A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .@.']../....."#.DY1\|+$..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 .T.J]../....."#.D...,$..A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....0.....0\r..m.....d...<.s....._keyhttps://rna-resource.acrobat.com/static/js/plugins/desktop-connector-files-select/js/plugin.js .7.e]../....."#.DQ.},$..A.....9Q].8O.z....=..:.N.{....N{.A..Eo.....A..Eo.....I=4.....

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):	2064
Entropy (8bit):	5.315048359672465
Encrypted:	false
SSDEEP:	24:Mfg1zZFufGMisp6r6C9QP8SHdqGpyMlKNpALhtwhUo4:h1zZ4+dsp61S9q/5/Qh6C3
MD5:	0E67AE8C64A4CC68D3DAA9D5A840B7C9
SHA1:	91348EC080EBF30BBE0A5777351C447DD4E63C90
SHA-256:	E99A7718DBE4D2409CB026EE7B0699E934495F6775FD0E9CA3B71FAF1CAC4C08
SHA-512:	95F1A38609A2E7990D0942FE58C8AB4CDFBC560700A9FFCF6E2443938C9ACA983EC15CF810CD69F75E2E148F5DFC60B287A78D5B581F3F5DE5335FBCE32189
Malicious:	false
Preview:	....h...oy retne....'.....'.....;.y~A..z.B_./.....*...z.B_./.....oB*.8.B_./.....#...(...A_./.....k7A..z.B_./.....D.4..z.B_./.....[.i..%..z.B_./.....<...W..J.8.B_./.....,+..._.#.z.B_./.....J..j....z.B_./.....6<|....8.B_./.....A?.2:...z.B_./.....+.{..'.z.B_./.....*)....J:.z.B_./.....2q....z.B_./.....P....V.z.B_./.....+.U.!..V.z.B_./.....P[. q.z.B_./.....!...0.o.z.B_./.....u\]..q.z.B_./.....z.B_./.....*.....z.B_./.....o..k...z.B_./.....^.~..z..z.B_./.....o..z.B_./.....Gy.'.h..z.B_./.....F..=z;..z.B_./.....3....z.B_./.....v...q...8.B_./.....C..M.....A_./.....a.....8.B_./.....~.,.4>..z.B_./.....&.S....z.B_./.....@..x..z.B_./.....=....m...z.B_./.....;/....z.B_./.....q..z.B_./.....MV3...z.B_./.....:..N.A...z.B_./.....B_./.0.....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):	292
Entropy (8bit):	5.141985365798705
Encrypted:	false
SSDEEP:	6:mrMA3NAVq2PWXp+N2nKuAl9OmbnIFUtpCMRAgZmwPCM0AlkwOWXp+N2nKuAl9Omt:SMA3OvaHAahFUtpCM7/PCMq5fHAaSJ
MD5:	F452A990C905B36C05AF8501BB98FCB5
SHA1:	B9DBEE00DEDB8B71D8E6059BBAB61DD6D68070DE
SHA-256:	FB82B31A71A2520A434EF6ED66C9460F6A4E74E3FFBC95624866E47F70568357
SHA-512:	D3FB404ED75B4BB484B87364922CB0985D786A51B81E769A2FA4C427B1B49280A8B3D888735B153123BA0D4EE2B9DD60ADF28CFE216D140CA15A0F1FE3372A21
Malicious:	false
Preview:	2021/02/22-21:20:40.054 1844 Reusing MANIFEST C:\Users\user\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache/MANIFEST-000001.2021/02/22-21:20:40.055 1844 Recovering log #3.2021/02/22-21:20:40.056 1844 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):	1835008
Entropy (8bit):	0.009659826032596219
Encrypted:	false
SSDEEP:	48:TGEiaGEiCsMi9sMiDgsMiDgsMiDdsMhCDOsMhCDo+sMhCDo+sMhCDo+sMhCDo+sW:trrCXonononononono
MD5:	21243F04C89A197BB6B7F6F83FC3143C
SHA1:	86C39801641D4689AF8792AFB690A0CADBE81263
SHA-256:	B71EB44A7471A903DEFF3A492C2981A68BFB32AB60A5D162E43364864DE135A3
SHA-512:	F36B2C48C1F0C30494202D6990352BF864F6D0EF073D8981C8033ECEDE9A0B55F90B422110C91DF95B7E714B5F7F1928FA75A64BFC2A9723234A7073AC945316
Malicious:	false
Preview:	VLnk.....?.....Tq.>..j.....

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210223052035Z-195.bmp	
Process:	C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe
File Type:	PC bitmap, Windows 3.x format, 152 x -152 x 32
Category:	dropped
Size (bytes):	92470

C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210223052035Z-195.bmp	
Entropy (8bit):	2.4797911135464776
Encrypted:	false
SSDEEP:	96:2LlVejFkwKrrYGh9CEVuPyVvHQgUArdUzGVtjKI/m4c1ztsD3xN+kXcpX:yejFgrYSVVVvcArawKlStGBNMpX
MD5:	FD99823E441BC036BF2017B4C9610DD2
SHA1:	8C6B6AC69DB74BA72F5BA1486DEE8A48D31CAFD3
SHA-256:	34A2CE5AF9EE1C986FA40F98BBCC8891DEA3BD1600946BE9CE82872F330A3C97
SHA-512:	0EAA6D9E09B46814A62DD7350D7630A7A8A174E5633C76A8DE8628A5C1DF5D000EE45173F5C6978EE674D200F2F9527E1DC61B065459DD84E871CCF11208855
Malicious:	false
Preview:	BM6i.....6...(.....h..... .....e...e...e...

C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5820	
Preview:	%!Adobe-FontList 1.16.%Locale:0x409..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Marlett.FamilyName:Marlett.StyleName:Regular.MenuName:Marlett.StyleBits:0.WeightClass:500.WidthClass:5.AngleClass:0.FullName:Marlett.WritingScript:Roman.WinName:Marlett.FileLength:27724.NameArray:0,Win,1,Marlett.NameArray:0,Mac,4,Marlett.NameArray:0,Win,1,Marlett.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:ArialMT.FamilyName:Arial.StyleName:Regular.MenuName:Arial.StyleBits:0.WeightClass:400.WidthClass:5.AngleClass:0.FullName:Arial.WritingScript:Roman.WinName:Arial.FileLength:1036584.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial.NameArray:0,Win,1,Arial.%EndFont..%BeginFont.Handler:WinTTHandler.FontType:TrueType.FontName:Arial-BoldMT.FamilyName:Arial.StyleName:Bold.MenuName:Arial.StyleBits:2.WeightClass:700.WidthClass:5.AngleClass:0.FullName:Arial Bold.WritingScript:Roman.WinName:Arial Bold.FileLength:980756.NameArray:0,Win,1,Arial.NameArray:0,Mac,4,Arial Bold.NameAr

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\Q68SRQ2E\fpt2.microsoft[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	127
Entropy (8bit):	4.913755802383416
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsehjAqTUWJVXWIfbxwDlJ53RSSPHFCqSRlAFKRKb:JFK1rUFihjAqTUW/Xbxwh/ESP4ngKwb
MD5:	4BBACE188DAE93BF36D5B9B4144DDA85
SHA1:	588380E8D889CC4B662CE91D1B72050F72753F0C
SHA-256:	08726ED7E931EC15FA4EB8512BF1D60DFEE0E7AA21FEF98985DA350BAA25B839
SHA-512:	1E1C609104CDB9E23C8D18A91CB1820E8E181E3716DEA7507868D4FC545474FFFFC1A052273732400224A2D0B599F34DB96C7E5760D8C6D167D0622BD7A14CD
Malicious:	false
Preview:	<root></root><root><item name="MUID" value="6131a93a-59cc-4c23-9829-d505c29eefbf" ltime="3547771792" htime="30869923" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{FC9A1D24-7596-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	32856
Entropy (8bit):	1.851632701505614
Encrypted:	false
SSDEEP:	384:rqTAxAbcAbB9AbBPAbBETAbBEw7AbBNVwvAbBNywoAbBNyuJAbBNyuE:d
MD5:	09500B9E8724D9268C8C87D88C230373
SHA1:	6473D54A7E256CB4147F301A4EB608004EF8BE81
SHA-256:	1D3CEB5A80D73942045735DDBAC2C91133C40688E99CF813292940FB0CF03F10
SHA-512:	DEBA0F6EA8DA1E191433D27E38C9607B8C6763D015A1E3CA08F05428E7A51F079F56890DDF2D2505A826D2F023D732993F12C3793113AB8F5E820F448993F0BA
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{042B8C2A-7597-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.565524770452342
Encrypted:	false
SSDEEP:	48:IwzGcpr+Gwpa47G4pQ4GrapbSkGQpKCG7HpRgTGIpG:rJZ2QM6GBS8AtT0A
MD5:	F8222DAC264A9003713F9065A8DBEF9A
SHA1:	04ECEE3E91DF5CC2BF883C40092DFE1F719B60AB
SHA-256:	6F9BD976A762AEE2B56810B6FA7C2B6852E0FABF8CD3542242CD9BB66EA2FC61
SHA-512:	B764C5D91E88B3A84DBEF3CFCCB42C6DFDA65992B3CAC8395D3FC190F8C8F596DD5E9F1C31B774E4B89B1C1B5370EEDD864B07450FB49E5B5C11673256E777D
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FC9A1D26-7596-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	310018

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FC9A1D26-7596-11EB-90E4-ECF4BB862DED}.dat	
Entropy (8bit):	3.7270474237289335
Encrypted:	false
SSDEEP:	6144:h7puBp2/bl8JT7puBp2/bl8JKzHlPBAIKCaYcwZAALpf:h7puBUl8Z7puBUl8S
MD5:	A7A5C9938F25B307DF268B6958DC1099
SHA1:	C0364F40FF16981C4B60ADAD61E1C654E0BFFF4E
SHA-256:	654C86A6DAE6F3594AD880013E1F255785DC6E9C21D850F8EB64B5D4672D5360
SHA-512:	BC3ADAFD879B6FC4914B452E379556D2A29E76C6D02AB255BD3CCEE23F7D4771B08AC10EBDCB4C26EBFFFEC6A47CEBD5B73EFE67C89CD2AE5F5FDF19DDA2162B
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.055582916560374
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE3nWimI002EtM3MHdNMNxOE3nWimI00ObVbkEtMb:2d6NxOmSZHKd6NxOmSZ76b
MD5:	51579DDB6E978A8DE62040F387B35140
SHA1:	0EDF1CEB701B8D370823B892605BFBCD9EFFCFC4
SHA-256:	979232D420315F5641F280732837BE71291281145DA63314DA296EEFC0754357
SHA-512:	F1B5AEB89C88F0295BC0647B2906AE6F2F73B5F89A63B92E3BC96230E13274D9CE8835B46992798E76308630C40AAA1AD8ED27E5F8F7B5698F3B9BA90898EF35
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xd371f790,0x01d709a3</date><accdate>0xd371f790,0x01d709a3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xd371f790,0x01d709a3</date><accdate>0xd371f790,0x01d709a3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.1006158707906355
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2k5mCmmnWimI002EtM3MHdNMNxe2k5mCmmnWimI00Obkak6EtMb:2d6NxrymCmmSZHKd6NxrymCmmSZ7Aa7b
MD5:	64DF3C1D1EA9747D29E06C94FE921B9B
SHA1:	05C7EB6B07FDD69D7AB7B73F75CA63B0745D40AE
SHA-256:	2D537448DC92CCD980C5D23134976CC43D8D29BBA916AC85B85868CE3E55D5FA
SHA-512:	747E808D7D9A2896C37ED4557D84365667158D4F8BC3FB2E7CA325B0C8BE8D105A95885B73B7535C13D4CF6BEC38C8AC214963D2A1D76ED8F8B0249CA004B4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xd3660bbd,0x01d709a3</date><accdate>0xd3660bbd,0x01d709a3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xd3660bbd,0x01d709a3</date><accdate>0xd3660bbd,0x01d709a3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.07379736559764
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL3nWimI002EtM3MHdNMNxvL3nWimI00ObmZEtMb:2d6NxvjSZHKd6NxvjSZ7mb
MD5:	53BE2FF06EF159107FED352BDE002BC3
SHA1:	1767793B74DFEE56A48CF6937641886BFEB687C1
SHA-256:	A327E217E98FF4E4E1CE33BF78F7EA16298A261F159A2BBB69346E54F08B9136
SHA-512:	1107086A5DC403E4219E4C2A008830AC1A80DA920C79E98EC69E3D5168F280AD2A1C8A393BF7AB465D99853B307BCA81AC529E0817911DC0F2D3880DE338522
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xd371f790,0x01d709a3</date><accdate>0xd371f790,0x01d709a3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xd371f790,0x01d709a3</date><accdate>0xd371f790,0x01d709a3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.092535848769221
Encrypted:	false
SSDEEP:	12:TMHdNMNxidJVosJVomnWimI002EtM3MHdNMNxidJVohnWimI00Obd5EtMb:2d6Nx2bosbomSZHKd6Nx2bohSZ7Jjb
MD5:	F42D4F0FCB490B7B6FEBBF708E5EC197
SHA1:	A9E339AB8A9159EBCC5E976928264D4232DCAC1F
SHA-256:	31DA500AF1478774E6EE8ADED122F1F119B848124512D4A5DF91BAA4DA4A41D3
SHA-512:	04D0F40203F0A63AF49BAB24F7BF4A27FBFDA2741B5768D165B5CA9572B9E78EC91C63D885D49C9725490E73A01BCDABC05E4BD58D669BEEE296ED2029F3BDCF
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xd3686e1d,0x01d709a3</date><accdate>0xd3686e1d,0x01d709a3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xd3686e1d,0x01d709a3</date><accdate>0xd36ad079,0x01d709a3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.090345402924196
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw3nWimI002EtM3MHdNMNxhGw3nWimI00Ob8K075EtMb:2d6NxQKSZHKd6NxQKSZ7YKajb
MD5:	B4A395008B0355CA67DFAEE3A2C74162
SHA1:	FA37248D80C45D6C9463A3D8DFA4846182E5818E
SHA-256:	A1B0A781A9976EB925F8323FDB9EBDD5BA82405BE3B1A4DE95A8E59BC19A7987
SHA-512:	D9BE2883578D4ADD58B0E12CE222F54995CF16109AC0A6D5C41EC63A1865D38F1C99208BDFC6F88748DBD7CF528F53A569060ED5C6D3771623146DDCE15F99
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xd371f790,0x01d709a3</date><accdate>0xd371f790,0x01d709a3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xd371f790,0x01d709a3</date><accdate>0xd371f790,0x01d709a3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.078044034673806
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nLe4nWimI002EtM3MHdNMNx0nLe4nWimI00ObxEtMb:2d6Nx0BSZHKd6Nx0BSZ7nb
MD5:	0C57438586C29FE6BC04963ECA6AB8D5
SHA1:	0873983EF31CC1321C7A02DF15D150D04E0DF981
SHA-256:	F053D3835EBC53112368B0794E33BBAA350F5C406171847574C04DB7928071F6
SHA-512:	D5D5A5FA5919512A59B88AE364292F65043145FACA3975C55B42238E8CBED8A2420530BA2AAE60FCE2DA7BDCB722525CBFA2546553F13808EFC39489A5D0FDFB
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xd36f95a0,0x01d709a3</date><accdate>0xd36f95a0,0x01d709a3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xd36f95a0,0x01d709a3</date><accdate>0xd36f95a0,0x01d709a3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.117807054022758
Encrypted:	false
SSDEEP:	12:TMHdNMNxxLe4nWimI002EtM3MHdNMNxxLe4nWimI00Ob6Kq5EtMb:2d6NxbSZHKd6NxbSZ7ob
MD5:	482BA8126210C09E154FC95D70F007B2
SHA1:	ACBD421F979637E00C111B076AAD0C7C6FA5BB1B
SHA-256:	D716FC89D829D949FD1F8AC64A7781C2AB84AC4CD69D756EBC9AE31838424E78
SHA-512:	CA27E559AE2A8D160E1BC1E95B01ABC42AD449E186D78BB373FBD5CA1AD6E076F48AF34113C67D3DFAF8971F4857983299D4E29898C4684CFC09BB68AF5A190
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xd36f95a0,0x01d709a3</date><accdate>0xd36f95a0,0x01d709a3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xd36f95a0,0x01d709a3</date><accdate>0xd36f95a0,0x01d709a3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.098529824807038
Encrypted:	false
SSDEEP:	12:TMHdNMNxcdJVosJVomnWimI002EtM3MHdNMNxcdJVosJVomnWimI00ObVEtMb:2d6Nx0bosbomSZHKd6Nx0bosbomSZ7Db
MD5:	9D3A444D531A9870EE23DC96113E1761
SHA1:	1E412540D3D22CE13351849F9F9841B489031B7C
SHA-256:	CA014D8F3C6B9E83CAB846054E18614F376BE8866B5726FDC0B4C878AC9658B0
SHA-512:	E9025D172D5F0E4369342F4F732FB4DCD2F2FF11625887E4E51AB91BB27F65D41314B7F87B697036470354E105E72F09D71A5ECF02B7DEF0A029C2845AF6A588
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xd3686e1d,0x01d709a3</date><accdate>0xd3686e1d,0x01d709a3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xd3686e1d,0x01d709a3</date><accdate>0xd3686e1d,0x01d709a3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.0790445478564425
Encrypted:	false
SSDEEP:	12:TMHdNMNxfndJVosJVomnWimI002EtM3MHdNMNxfndJVosJVomnWimI00Obe5EtMb:2d6Nx1bosbomSZHKd6Nx1bosbomSZ7i/
MD5:	F8F1A3DFAB7BB7D8AE3EFFA4AB792732
SHA1:	D382A0C78E916803D3C091633E777302270476E8
SHA-256:	F582E05C51644A2EBEFBF2A79E316736722BEBB35353DA63262BF58B8DDF1F4D
SHA-512:	2A13DB9436B55F141E35567452B463CA60B67FC9D29DC8A95325B8E2CDCE230E89C6FBD332ACF2CC490D9E0B0C88B88B84458D8E95F9700E1B41B48A8C9798A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xd3686e1d,0x01d709a3</date><accdate>0xd3686e1d,0x01d709a3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xd3686e1d,0x01d709a3</date><accdate>0xd3686e1d,0x01d709a3</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	72284
Entropy (8bit):	3.078603703450606
Encrypted:	false
SSDEEP:	48:sT5gT5FT5dT5YgyyyyyyyyyyyydT5KYT5/QQQQQ0O/5O/oO/AO/bgyyyyyyyyyM:+gzzIb9QQQQQMQQQQQQQQQQAQQQQQJ
MD5:	8FCD21D6C9B3258B6E9D2D54E965AA41

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
SHA1:	181981C0CCBA3B742DD03BD76A1F7355104B7A77
SHA-256:	E70DD6945DAD5D686ADF1D4C545C5E0556057CD5C0374C50C4C4B8C5B93AB360
SHA-512:	02284FF3DF9B1572C36102F5BDBF19370D0FEBA733FE1C9CEE5D07096FC755E8BC6C26A87B5D473986A651BD78AD84C771B78179674D73FC6EFCF3C3BDA74A7
Malicious:	false
Preview:	W.h.t.t.p.s.:././.a.a.d.c.d.n...m.s.a.u.t.h...n.e.t./.e.s.t.s./.2...1./.c.o.n.t.e.n.t./.i.m.a.g.e.s./.f.a.v.i.c.o.n._.a._.e.u.p.a.y.f.g.g.h.q.i.a.i.7.k.9.s.o.l.6.l.g.2...i.c.o.~(.....h(.....(.....(.....("P.....""""""

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\arrow_px_up[1].gif	
SHA-512:	B17552D90D0038531A5F4E78DA553F9109346CB25851F38996BFAB54906A898DE848FEFFD31E8D0BF0A32D956513CA7ED72D2F4C3AE47922C6F9D370584288EF
Malicious:	false
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/arrow_px_up.gif?version=27f11222-771f-bb95-a744-f0b962f89b91
Preview:	GIF89a.....3..... ....!.....,..... ..... .`.....\8....!>L(.b@.;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\favicon_a_eupayfgghqiai7k9sol6lg2[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeeekzgsLsLsLsLsQZp:nfgyyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0
Malicious:	false
IE Cache URL:	http://https://aadcdn.msauth.net/ests/2.1/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico
Preview:	.....h(..f...HH.....(..00.....h....6.. .....=.....@.....(....A..(.....(.....''P.....''''''

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2[1].svg	
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0, 0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.61 1,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.9 52,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\override[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	1531
Entropy (8bit):	4.797455242405607
Encrypted:	false
SSDEEP:	24:Udf0F+MOu2UOqD3426TKgR2Yyk9696TkMYqdfskeEkeGk/ksuF9qaSm9qags:Ud8FYqTj36TKgR2Yyk9696TkMYO0keEW
MD5:	A570448F8E33150F5737B9A57B6D889A
SHA1:	860949A95B7598B394AA255FE06F530C3DA24E4E
SHA-256:	0BD288D5397A69EAD391875B422BF2CBDCC4F795D64AA2F780AFF45768D78248
SHA-512:	217F971A8012DE8FE170B4A20821A52FA198447FA582B82CF221F4D73E902C7E3AA1022CB0B209B6679C2EAE0F10469A149F510A6C2132C987F46214B1E2BBBC
Malicious:	false
IE Cache URL:	http://https://statics-marketingsites-eus-ms-com.akamaized.net/statics/override.css?c=7
Preview:	a.c-call-to-action:hover, button.c-call-to-action:hover{box-shadow:none!important}a.c-call-to-action:hover span, button.c-call-to-action:hover span{left:0!important}...c-call-to-action:not(.glyph-play):after { right: 0!important;} a.c-call-to-action:focus,button.c-call-to-action:focus{box-shadow:none!important}a.c-call-to-action:focus span,button.c-call-to-action:focus span{left:0!important;box-shadow:none!important}...theme-dark .c-me .msame_Header_name {color: #f2f2f2;}...pmg-page-wrapper .uhf div, .pmg-page-wrapper .uhf button, .pmg-page-wrapper .uhf a, .pmg-page-wrapper .uhf span, .pmg-page-wrapper .uhf p, .pmg-page-wrapper .uhf input {font-family: Segoe UI, SegoeUI,Helvetica Neue,Helvetica,Arial,sans-serif !important;}..@media (min-width: 540px) {.pmg-page-wrapper .uhf .c-uhfh-alert span, .pmg-page-wrapper .uhf #uhf-g-nav span, .pmg-page-wrapper .uhf .c-uhfh-actions span, .pmg-page-wrapper .uhf li, .pmg-page-wrapper .uhf button, .pmg-page-wrapper .uhf a, .pmg-page-wrapper .uhf #meC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\script[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	50466
Entropy (8bit):	5.403327253117392
Encrypted:	false
SSDEEP:	768:3Vs4A3c/bSKCzUm4D19h3j9UIAyjYXQgyjYXEoygRRsRnMtoafRnvdMIKebqH:h6c/bSKCzUm4DDh3j+9XQ4XE+BZdMIK9
MD5:	633B23CA8A850C508C146635DB4239F5
SHA1:	CF78DA53BD7561F3ACB33710016ECBF60E9F0204
SHA-256:	DAA1677D2640BE8A77F6C69EEE3911D2F8CF81DAA7BB604800A2D63A8F130C95
SHA-512:	82D4887AB9BB6A449FB0E5B6DEF80215B5F9E51058DCB1B8B7CD583A880F93428C3FB75B37C0E9481843203A4878FEF32424B5CD2EBCDD811D92604A1C1BCAB
Malicious:	false
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=1a053411-4f63-d069-d3b8-11d5d720eeb4
Preview:	function ShowSelectedComponentKeyPress(n,t){if(window.event.keyCode==13)return ShowSelectedComponent(n,t),!1}function ShowHighLight(n){var t=$("#div"+n).height();$.browser.msie&&parseInt($.browser.version,10)==7?$("#div"+n+" > .highlight").css({width:"0",height:"0","background-color":"white",float:"left","border-top":Math.round(t/2+.3)+"px solid white","border-right":"0.75em solid "+$("#div"+n).css("background-color"),"border-bottom":Math.round(t/2+.3)+"px solid white"}):$("#div"+n+" > .highlight").css({width:"0",height:"0","background-color":"white",float:"left","border-top":t/2+.3+"px solid white","border-right":"0.75em solid "+$("#div"+n).css("background-color"),"border-bottom":t/2+.3+"px solid white"})}function SetRightSideNavigationMenuHeight(){$("[id^=dvModuleGroup_]").hide();window.location.search.toLowerCase().indexOf("bookmarkid")!=-1&&SelectBookMark();window.location.search.toLowerCase().indexOf("componentid")!=-1&&LoadSelectedInternalLink();$(".div_side_comp").length>0&&$(".

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\script[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	121249
Entropy (8bit):	5.258860505507024
Encrypted:	false
SSDEEP:	1536:+JXd+YOlaYOyguxH6GdXJKjZtQ3EBJ0PYmwYmEZeQ8Wt2Db7ACu8J8lvC7CQBgAc:ed+YOlaYOyguxHbdX2nX5PaCfey
MD5:	B110D87662D257F657ABCCEF7AF5CD09
SHA1:	FD7519D842B6344448E6F1D69DFFA5F896FAE4A6
SHA-256:	65E82E7414D88BC864191400084C24DA27052E7A61F9F3C1F1EFDFEE433D558C
SHA-512:	EF429EE8701D0748DE81CEE25D15C9674487691ACA8982F6D43DA519E1CDFD5082D9DE5A71D1FB457250828433856BAB4A2CE7E035152FE9C16224FA433D35D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\script[2].js	
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSScripts/script.jsx?k=0502864a-b6ef-2f14-9f8e-267004d3a4e0_c5ea3348-55af-729a-2641-14f0312bacf3_742bd11f-3d7c-9955-3df5-f02b66689699_cb9d43d2-fbae-5b5c-827f-72166d6b87fc_49488e0d-6ae2-5101-c995-f4d56443b1d8_7dea7b90-4334-c043-b252-9f132d19ee19_38aa9ffb-ddb5-75be-6536-a58628f435f5_e3e65a0a-c133-43e7-571d-2293e03f85e6_4ca0e9dc-a4de-17ba-f0de-d1d346cb99e2_06310cd8-41c6-3b11-4645-b4884789ed70_5c27e8aa-9347-969e-39ac-37a4de428a8d_d6872b5a-5310-a73c-7cb3-227a3213a1c5_be92d794-4118-193f-9871-58b72092a5ac_64c742e2-b29c-b6c1-fdd9-accf33ec40bd_cf2ceca9-3467-a5b3-d095-68958eee6d4c_cec39dd8-f1d3-56f1-abfc-a7db34ff7b46_ec5fa2c9-3950-ff57-a5c3-1fa77e0db190_d19f9592-65df-bcc9-e30e-439b875c3381_76a3d06f-f11f-77ef-9bfd-6227ba750200_5e1caa45-461c-3b04-f88b-8cd50af16db5_c2dceda8-20b4-7d3f-13b6-9cac67d7df17_914fa41b-cc86-d3b0-4e15-2fdfa357bcc7_40c6c884-da6e-7c2c-081f-4a7dfe7c7245_ae79ba96-1a9d-debd-a5b1-f3067213b9b8
Preview:	function getQueryValue(n,t){var r=new RegExp("[\\?&]"+t+"=([^&#]*)","gi"),i=r.exec(n);return i==null?"":decodeURIComponent(i[1].replace(/\+/g," "))}function getStore(n){var t="ClosestStore.asmx",r,i;$(".store-geo[data-GeoStoreLocalServiceURL]").length&&(t=$(".store-geo").first().attr("data-GeoStoreLocalServiceURL"));i="POST";typeof n!="undefined"&&(r={latitude:JSON.stringify(n.coords.latitude),longitude:JSON.stringify(n.coords.longitude)},t=t+"ClientGeo",i="GET");$.ajax({url:t,type:i,timeout:5e3,data:r,contentType:"application/json; charset=UTF-8",dataType:"json",error:function(){$(".store-geo").remove();$(".store-editorial").fadeIn(1e3)},success:function(n){if(typeof n!="undefined"&&typeof n.d!="undefined"&&typeof n.d.City!="undefined"&&n.d.City!=""&&n.d.StoreUrl!="undefined"&&n.d.StoreUrl!=""){var t=$(".store-geo:first").text();$(".store-geo a").html(t+" "+n.d.City);$(".store-geo a").attr("href",n.d.StoreUrl);$(".store-editorial").remove();$(".store-geo").fadeIn(1e3)}else $(".store-g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wcp-consent[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	255440
Entropy (8bit):	6.051861579501256
Encrypted:	false
SSDEEP:	6144:PIgagvUI0iDsW9Whsredo7NjIZjIZP0aNWgF9Dyjzh:PIgaHI0iIUedo7NjIZjIZP0o74t
MD5:	38B769522DD0E4C2998C9034A54E174E
SHA1:	D95EF070878D50342B045DCF9ABD3FF4CCA0AAF3
SHA-256:	208EDBED32B2ADAC9446DF83CAA4A093A261492BA6B8B3BCFE6A75EFB8B70294
SHA-512:	F0A10A4C1CA4BAC8A2DBD41F80BBE1F83D767A4D289B149E1A7B6E7F4DBA41236C5FF244350B04E2EF485FDF6EB774B9565A858331389CA3CB474172465EB3EF
Malicious:	false
IE Cache URL:	http://https://wcpstatic.microsoft.com/mscc/lib/v2/wcp-consent.js
Preview:	var WcpConsent=function(e){var a={};function i(n){if(a[n])return a[n].exports;var o=a[n]={i:n,l:!1,exports:{}};return e[n].call(o.exports,o,o.exports,i),o.l=!0,o.exports}return i.m=e,i.c=a,i.d=function(e,a,n){i.o(e,a)||Object.defineProperty(e,a,{enumerable:!0,get:n})},i.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},i.t=function(e,a){if(1&a&&(e=i(e)),8&a)return e;if(4&a&&"object"==typeof e&&e&&e.__esModule)return e;var n=Object.create(null);if(i.r(n),Object.defineProperty(n,"default",{enumerable:!0,value:e}),2&a&&"string"!=typeof e)for(var o in e)i.d(n,o,function(a){return e[a]}.bind(null,o));return n},i.n=function(e){var a=e&&e.__esModule?function(){return e.default}:function(){return e};return i.d(a,"a",a),a},i.o=function(e,a){return Object.prototype.hasOwnProperty.call(e,a)},i.p="",i(i.s=1)}([function(e,a,i){window,e.exports=function(e){var a={};function i(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\17-f90ef1[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	134136
Entropy (8bit):	5.224428921008954
Encrypted:	false
SSDEEP:	3072:1f/HuFVppxvIeq0i9d1EwgXA95Ki5DCE4t:1f/Hu/FIhRwt
MD5:	D567746F6D3BABF05ACF7A63730AC2CB
SHA1:	DDB8B9E24115D9653C432C1C2A3C57E0F881AFEB
SHA-256:	F4DF01A10175F31D0620AE8AA24854DF0D8DCB0C752E8465376B2ED3DEF62DE0
SHA-512:	3F9F18CD40F4CDCDA4F55174AC02766F4F511A61797296D59F1F216E2A51FC9068981E0C41C998ECB05053495BD7971FEA56A032F5438438A224CCA1A33F7189
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-eus-prod/shell/_scrf/js/themes=default/54-af9f9f/c0-247156/de-099401/e1-a50eee/e7-954872/d8-97d509/f0-251fe2/46-be1318/77-04a268/11-240c7b/63-077520/a4-34de62/bb-d7480b/db-bc0148/dc-7e9864/6d-c07ea1/29-1ec5a9/f6-aa5278/cd-23d3b0/6d-1e7ed0/b7-cadaa7/c4-898cf2/ca-40b7b0/4e-ee3a55/3e-f5c39b/c3-6454d7/f9-7592d3/92-10345d/79-499886/7e-cda2d3/69-13871c/e5-08f1c0/e0-3c9860/91-97a04f/1f-100dea/33-abe4df/17-f90ef1?ver=2.0&iife=1
Preview:	(function(){/**. * @license almond 0.3.3 Copyright jQuery Foundation and other contributors.. * Released under MIT license, http://github.com/requirejs/almond/LICENSE. */.var requirejs,require,define,__extends;(function(n){function r(n,t){return w.call(n,t)}function s(n,t){var o,s,f,e,h,p,c,b,r,l,w,k,u=t&&t.split("/"),a=i.map,y=a&&a["*"]||{};if(n){for(n=n.split("/"),h=n.length-1,i.nodeIdCompat&&v.test(n[h])&&(n[h]=n[h].replace(v,"")),n[0].charAt(0)==="."&&u&&(k=u.slice(0,u.length-1),n=k.concat(n)),r=0;r<n.length;r++)if(w=n[r],w==="."")n.splice(r,1),r-=1;else if(w===".."){if(r===0||r===1&&n[2]===".."||n[r-1]===".")continue;else r>0&&(n.splice(r-1,2),r-=2);n=n.join("/")}if((u||y)&&a){for(o=n.split("/"),r=o.length;r>0;r-=1){if(s=o.slice(0,r).join("/"),u)for(l=u.length;l>0;l-=1)if(f=a[u.slice(0,l).join("/")],f&&(f=f[s],f)){e=f;p=r;break}if(e)break;!c&&y&&y[s]&&(c=y[s],b=r)}!e&&c&&(e=c,p=b);e&&(o.splice(0,p,e),n=o.join("/"))}return n}function y(t,i){return function(){var r=b.call(arguments,0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Clear[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	2885
Entropy (8bit):	5.681418867892512
Encrypted:	false
SSDEEP:	48:t1XXw+kOhX/BxVgnK/Q6GiuGq9juwbae13NhcKBLd4YNKklqS6r0qQJcF1mEIIQX:H9W3iuV96wDrHBZ4YTqroqQmO1niz6
MD5:	1E0FF548B77453D165DAB1D679DED5C2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Clear[1].htm	
SHA1:	EAF2BB58DB64B88401D26E5EBDDE3D87BBB10C02
SHA-256:	E8C5016629BFE83A55BBFDF2666EF5D6AF8EB830DCF1CA748C1C0FD7ECC9AFBF
SHA-512:	D6A9CDC9F1ABBD6EC149020227AA0ED1E23DD85DFE3C87696C7CC48CDDD3AC8051725E58746482AE63450CD171DEB47CC0F51100A6E0EADC08B8530849425F7
Malicious:	false
IE Cache URL:	http://https://fpt2.microsoft.com/Clear.HTML?ctx=Ls1.0&session_id=0656ef1f3f31449c938682f87c100e08&id=6131a93a-59cc-4c23-9829-d505c29eefbf&w=8D8D76F84C51145&tkt=taBcrIH61PuCVH7eNCyH0FC0izOzUpX5wN2Z%252b5egc%252f4JBZtUcMYOlunrxuKLGmwGT22%252fQT4CLtoaLEZ%252bAFiSyQdxVjWMyLkmJx%252f9h8znkxUN2kTp0zDN0%252fhXYH9YdFfTmXDiYG3GhD6hNBHJ%252bLCMbtYpgolqOmOFBDQUs%252fuwajkmYA7osUMKNyW54H4sVI5zx%252f6MlCi4Hw5Hy3%252fr8H5jpa23m3c5yf2F4mu8q2zCqCUa%252f0DsHoYcDoVTerQYjLUJn2%252bULY91sDiJCcgsC9TxOUcZpdJ3evIiXV8If5CTJ4Y%253d&CustomerId=33e01921-4d64-4f8c-a055-5bdaffd5e33d
Preview:	<!DOCTYPE html>..<html xmlns="http://www.w3.org/1999/xhtml">..<head>.. <title></title>..</head>..<script>function BaseStamp() { this.GetStorageQsInfo = function () { if (window.localStorage) { var n = window.localStorage.getItem(lsKey); var lsupd = "False"; if (lsupd === "true" && n) { var xhr = new XMLHttpRequest(), method = "GET", url = target + "updatels.html?ofid=" + n + "&session_id=" + sid + "&CustomerId=" + cid; xhr.open(method, url, true); xhr.onreadystatechange = function () { if (xhr.readyState === XMLHttpRequest.DONE && xhr.status === 200) { var update = xhr.responseText; if (update && update.toLowerCase() === "true") { window.localStorage.setItem(lsKey, id); } } }; xhr.send(); } if (n && n != null && n != "" || (window.localStorage.setItem(lsKey, id), n = id), id != n) return "session_id=" + sid + "&CustomerId=" + cid + "&fid=" + id + "&ofid=" + n + "&w=" + ticks + "&auth=" + encodeURIComponent(authKey) } return "" }; this.newXMLHttp = function () { var n = null; return

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Print[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	476
Entropy (8bit):	7.35124642782842
Encrypted:	false
SSDEEP:	12:6v/78/8QCeKXzjl5V6VQTdwbtsxET1SDQi7N:sNfF6VYd6tf1SdN
MD5:	B8E8859FCD4E43D51233559C17A3C7BD
SHA1:	F0CA023F26A84761995FA0BF6935DE6A3B8AE6F8
SHA-256:	DC15A37B4015D0DECF639006E4F9002E742DDBFD7C669EC0AE469057F238B78D
SHA-512:	3605E4C4FE22E6E05553F89D34CFE8B3E5CA72FBDADCCD8B279835A0ECEFCD10B1BF2AD1ACCEEB168EE369E23A8AD205720FBF33A184188A7F23AEA7B0F22005
Malicious:	false
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSImages/Print.png?version=03620f3a-5d1e-5a73-a117-a2f71eee437d
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....IDAT8O.S;..A.....M6.4....@.47....^I..<."&..W..Y...Y.....m...E.<..$..n...j..kL&.....}.j.....)@.....r..Q....]. .+.w...f3.R)...2^...ddO.^..Ud.BE..*D..h...!.....h..p..t...9.....1.."tD.....y.h.AQ.{."...J.D.U....c.b.i.h.t:..$&q..J..n.+9.r..B..F...e..`<...oS....Z-.H....NG...Jl..D.Z..@!...s<....m.'Ll..vc.?..~..v.n.9.;.m.5..K.A .....z=../>...M....r9..~...*..go.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\QVMJZWO9.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	21443
Entropy (8bit):	5.800691650258718
Encrypted:	false
SSDEEP:	384:HzWb0IEsQdsQvZxyF1Aw8WqyvW+dnwCIUTlLI2M/zvyMEZWpS:T5H9yF1IWqCdPlG/2d5
MD5:	FB5E24C92D52CA4DFC167D7355DB4D5C
SHA1:	AE724762B16EB843E183500FF015711AF85C3035
SHA-256:	2C6BAC01C706CB754518FF23E42394D122018A42F250049931AF372F19BAB45A
SHA-512:	819C7E86A955E96E0C4A0C1555CFE8DB65FA9C37F7BD31D0410D67F4D12B8F2E855DB0153EFE7E8637D23B65C80E64BE566F9F690A1B7C4A027B8AF5A064150
Malicious:	false
IE Cache URL:	http://https://fpt.live.com/?session_id=0656ef1f3f31449c938682f87c100e08&CustomerId=33e01921-4d64-4f8c-a055-5bdaffd5e33d&PageId=SU&mkt=EN-US&ru=https%3a%2f%2flogin.live.com%2foauth20_authorize.srf%3flc%3d1033%26response_type%3dcode%26client_id%3d51483342-085c-4d86-bf88-cf50c7252078%26scope%3dopenid%2bprofile%2bemail%2boffline_access%26response_mode%3dform_post%26redirect_uri%3dhttps%253a%252f%252flogin.microsoftonline.com%252fcommon%252ffederation%252foauth2%26state%3drQIIAeNisNLJKCkpKLbS1y_ILypJzNHLzUwuyi_OTyvJz8vJzEvVS87P1csvSs9MAbGKhLgE5N-HsRnaz3GZ3Nb0o0aAj2MWI2d8TmYZWOUqRmXCxulfYGR8wch4i0nQvyjdMyW82C01JbUosSQzP-8Ci8ArFh4DZisODi4BBgkGBYYfLIyLWIG2Rik0X16_dbXTrqAUuYQeZ4ZTrPpRVd4W-b7mmV4ppv5hlW6-lqaluRYWHrl5XtppBkXhQUUhmQElZWVGAaGBtqZWhhPYhCawMZ1iY_jAxtjBznCAk_EWl4iRgaGlroGRroGJgoGllZGRlbFRFAA1%26estsfed%3d1%26lw%3d1%26fl%3deasi2%26fci%3dhttps%253a%252f%252fportal.microsoftonline.com.orgid.com%26mkt%3dEN-US%26uaid%3d0656ef1f3f31449c938682f87c100e08
Preview:	<!DOCTYPE html>..<html xmlns="http://www.w3.org/1999/xhtml">..<head>.. <title></title>.. <script>var localTarget="https://fpt.live.com/",target="https://fpt2.microsoft.com/",txnKey="session_id",txnId="0656ef1f3f31449c938682f87c100e08",ticks="8D8D76F84C51145",ridKey="id",rid="6131a93a-59cc-4c23-9829-d505c29eefbf",lskey="MUID",authKey="taBcrIH61PuCVH7eNCyH0FC0izOzUpX5wN2Z%252b5egc%252f4JBZtUcMYOlunrxuKLGmwGT22%252fQT4CLtoaLEZ%252bAFiSyQdxVjWMyLkmJx%252f9h8znkxUN2kTp0zDN0%252fhXYH9YdFfTmXDiYG3GhD6hNBHJ%252bLCMbtYpgolqOmOFBDQUs%252fuwajkmYA7osUMKNyW54H4sVI5zx%252f6MlCi4Hw5Hy3%252fr8H5jpa23m3c5yf2F4mu8q2zCqCUa%252f0DsHoYcDoVTerQYjLUJn2%252bULY91sDiJCcgsC9TxOUcZpdJ3evIiXV8If5CTJ4Y%253d",IsInfo=true,cid="33e01921-4d64-4f8c-a055-5bdaffd5e33d",splitFonts=false,pageId="SU",pushEnv="";(function(){function c(){var i=0,n;return t&&t.length&&(i=t.length),n="",window.ActiveXObject?(n+="plugin_flash=false",n+="&plugin_windows_media_player=false",n+="&plugin_adobe_acrobat=false",n+="&plugin_silve

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\app[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\app[1].css	
Size (bytes):	262641
Entropy (8bit):	4.9463902181496096
Encrypted:	false
SSDEEP:	3072:u+Vd0pBbqPLYoyjFkxD2hAYwJb8ILm731Ss:u+Vd0DePLYoyjFkxD2hAYwJbZLM31Ss
MD5:	7C593B06759DB6D01614729D206738D6
SHA1:	0D4F76D10944933B8DDECFFE9691081439A77A3C
SHA-256:	F7D9FB0479DE843CF3FB0B78FC56BBB9E30BF0A238C6F79D9209FA8B22EFB574
SHA-512:	EF91B610CF17A17AAFB48984B4403EF175EB86096E3F12E23AE8D4C7C96EF60ED14DA3F69721E095CD2ACE3F0A06190186D000992823814BB906F7FB3576C2C1
Malicious:	false
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/external/oneui/oneui1.16.2/dist/css/app.css
Preview:	@font-face {. font-family: "wf_segoe-ui_normal";. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot");. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot?#iefix") format("embedded-opentype"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.woff") format("woff"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.ttf") format("truetype"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.svg#web") format("svg");. font-weight: normal;. font-style: normal; }..@font-face {. font-family: "wf_segoe-ui_light";. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.eot");. src: url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.eot?#iefix") format("embedded-opentype"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.woff") format("woff"), url("//i.s-microsoft.com/fonts/segoe-ui/west-european/light/latest.ttf") format("truetype

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\converged.v2.login.min_wixdbz3ubznoegxpcgkfog2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	108310
Entropy (8bit):	5.291533401897737
Encrypted:	false
SSDEEP:	1536:QpHDglkuhw+ExiazA/PWrF7qvEAFiQcpmaB9sG6yVUnT:lEBgyVUT
MD5:	5A25DD6F3DD40593681065E908691FA2
SHA1:	2F0D8A2C1C76B8B6D5354240907D353701AA11B7
SHA-256:	A96B2B12489A80EAFE62CC4BCC04CB367E2B54EFC3039E484211C7DEEC12C0B8
SHA-512:	56891213289085B23A6811CAD91B4E64F8B4D15A704DE9781246BCC1488AE8D9F89FFE8502EA62E7A0C9324133CAE0ED07C71F6016FFAB4070E3055B7C8135D5
Malicious:	false
IE Cache URL:	http://https://aadcdn.msauth.net/ests/2.1/content/cdnbundles/converged.v2.login.min_wixdbz3ubznoegxpcgkfog2.css
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. *//*!---------- START OF THIRD PARTY NOTICE ----------..This file based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise...//----------.twbs-bootstrap-sass (3.3.0).//----------..The MIT License (MIT)..Copyright (c) 2013 Twitter, Inc..Permission is hereby granted, free of charge, to any person

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ellipsis_635a63d500a92a0b8497cdc58d0f66b1[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	900
Entropy (8bit):	3.8081778439799248
Encrypted:	false
SSDEEP:	24:t4CvnAVRHf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUV0UFl:fn+1QqC4GuiHFXS1QqCWRHQ3V1QqCWRV
MD5:	635A63D500A92A0B8497CDC58D0F66B1
SHA1:	A32EBA4B4D139E8DA52C5801A13C1EE222B2B882
SHA-256:	61D7CCC5D2C41BF86BE6CEFB0063405067849BA64E9F219F60596EF09A54A942
SHA-512:	EFFE15E105FC5FA853E76917B533AAE6C75EBA9A256049FB5EAB88BBF319D63A4CE4AE3743A09D6A5F474B01649D6EDC5C8BCCC61B8CA9EA9E5C39E7AE724C16
Malicious:	false
IE Cache URL:	http://https://aadcdn.msauth.net/shared/1.0/content/images/ellipsis_635a63d500a92a0b8497cdc58d0f66b1.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089,1.107,1.107,0,0,1-.446-.089M8,6.857m6.857,0a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,8,6.857m6.857,0a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089,1.107,1.107,0,0,1-.446-.089,1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893,1.164,1.164,0,0,1,.607-.607A1.107,1.107,0,0,1,8,6.857Z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	915
Entropy (8bit):	3.8525277758130154
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c[1].svg	
SSDEEP:	24:t4CvnAVRfFArf1QqCSzGUdiHTVtpRduf1QqCWbVHTVeUV0Uv6f1QqCWbVHTVeUVx:fn1r1QqC4GuiHFXS1QqCWRHQ3V1QqCWz
MD5:	2B5D393DB04A5E6E1F739CB266E65B4C
SHA1:	6A435DF5CAC3D58CCAD655FE022CCF3DD4B9B721
SHA-256:	16C3F6531D0FA5B4D16E82ABF066233B2A9F284C068C663699313C09F5E8D6E6
SHA-512:	3A692635EE8EBD7B15930E78D9E7E808E48C7ED3ED79003B8CA6F9290FA0E2B0FA3573409001489C00FB41D5710E75D17C3C4D65D26F9665849FB7406562A406
Malicious:	false
IE Cache URL:	http://https://aadcdn.msauth.net/shared/1.0/content/images/ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#777777" d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089A1.107,1.107,0,0,1,.7,9.054a1.164,1.164,0,0,1-.607-.607,1.161,1.161,0,0,1,0-.893A1.164,1.164,0,0,1,.7,6.946a1.107,1.107,0,0,1,.446-.089M8,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.893,1.164,1.164,0,0,1-.607.607,1.107,1.107,0,0,1-.446.089,1.107,1.107,0,0,1-.446-.089A1.107,1.107,0,0,1,6.857,8,1.107,1.107,0,0,1,7.054,7.7a1.164,1.164,0,0,1,.607-.607,1.161,1.161,0,0,1,.893,0,1.164,1.164,0,0,1,.607.607,1.107,1.107,0,0,1,.089.446,1.107,1.107,0,0,1-.089.446,1.164,1.164,0,0,1-.607.607,1.161,1.161,0,0,1-.893,0,1.164,1.164,0,0,1-.607-.607

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\shell.min[1].css	
SHA-256:	49E5166F40D8586714F86E08AB76A977199DF979357147A0E81980A804151C2A
SHA-512:	6669AE352FF46DB734BB8F973D1C0527C3A5EC4119D534AAE4C33F29EFF970168ED5FE200A05D4E1B6A2EC0E090E2207549B926317D489DC7664B0D9C208546
Malicious:	false
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/onestorerolling-1510-19009/shell/v3/scss/shell.min.css
Preview:	@charset "UTF-8";@font-face{font-family:'wf_segoe-ui_normal';src:local("Segoe UI");src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot");src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.eot?#iefix") format("embedded-opentype"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.woff") format("woff"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.ttf") format("truetype"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/normal/latest.svg#web") format("svg");font-weight:normal;font-style:normal}@font-face{font-family:'wf_segoe-ui_semilight';src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.eot");src:url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.eot?#iefix") format("embedded-opentype"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.woff") format("woff"),url("//i.s-microsoft.com/fonts/segoe-ui/west-european/semilight/latest.ttf")

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	137436
Entropy (8bit):	5.360850019087837
Encrypted:	false
SSDEEP:	1536:+Fk5W00zHVaAgrBmeZCstBwB/BxBf9e969j9S9h919g9Z9C9f9g9Z9e979Q9t9Vp:+Fk5W003MC/
MD5:	D0519383C16A2B2D2879BFBF15845F0C
SHA1:	B2FBBC365B2CA853B1CBEAAA0F10BB05148ED9AA
SHA-256:	046BA9FDD7992751785036A03AB6EDD3052465C23C2BAD1ADC80905DC6AA39A9
SHA-512:	2DB8E6E4AD75F756D0B70071EC49EA4FF54360AFDAAC007C0FFD5ACF575961E661DD275329347210AD71206885A50DA2E58F12CE84E6C7A3BC3D5EDD81E3B5BE
Malicious:	false
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSStyles/style.csx?k=3c9ade18-bc6a-b6bd-84c3-fc69aaaa7520_899796fc-1ab6-ed87-096b-4f10b915033c_e8d8727e-02f3-1a80-54c3-f87750a8c4de_6e5b2ac7-688a-4a18-9695-a31e8139fa0f_b3dad3e4-0853-1041-fa46-2e9d6598a584_fc29d27f-7342-9cf3-c2b5-a04f30605f03_28863b11-6a1b-a28c-4aab-c36e3deb3375_907fa087-b443-3de8-613e-b445338dad1f_a66bb9d1-7095-dfc6-5a12-849441da475c_1b0ca1a3-6da9-0dbf-9932-198c9f68caeb_ef11258b-15d1-8dab-81d5-8d18bc3234bc_11339d5d-cf04-22ad-4987-06a506090313_50edf96d-7437-c38c-ad33-ebe81b170501_8031d0e3-4981-8dbc-2504-bbd5121027b7_3f0c3b77-e132-00a5-3afc-9a2f141e9eae_aebeacd9-6349-54aa-9608-cb67eadc2d17_0cdb912f-7479-061d-e4f3-bea46f10a753_343d1ae8-c6c4-87d3-af9d-4720b6ea8f34_a905814f-2c84-2cd4-839e-5634cc0cc383_190a3885-bf35-9fab-6806-86ce81df76f6_05c744db-5e3d-bcfb-75b0-441b9afb179b_8beffb66-d700-2891-2c8d-02e40c7ac557_b1fe3f15-7512-0a8f-a55b-b316245621b5_f9c8eff0-3e34-2c33-6c0d-1fa7c5077eec
Preview:	@font-face{font-family:'wf_segoe-ui_light';src:url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.eot');src:local("Segoe UI Light"),local("Segoe WP Light"),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.eot?#iefix') format('embedded-opentype'),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.woff') format('woff'),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.ttf') format('truetype'),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/light/latest.svg#web') format('svg');font-weight:normal;font-style:normal}@font-face{font-family:'wf_segoe-ui_normal';src:url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/normal/latest.eot');src:local("Segoe UI"),local("Segoe"),local("Segoe WP"),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/normal/latest.eot?#iefix') format('embedded-opentype'),url('//c.s-microsoft.com/static/fonts/segoe-ui/west-european/normal/latest.w

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\2_vD0yppaJX3jBnfbHF1hqXQ2[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
IE Cache URL:	http://https://acctcdn.msauth.net/images/2_vD0yppaJX3jBnfbHF1hqXQ2.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144.2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-1017.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUnits="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\RE1Mu3b[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 216 x 46, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	4054
Entropy (8bit):	7.797012573497454
Encrypted:	false
SSDEEP:	48:zICvnyRHJ3BRZPcSPQ72N2xoiR4fTJX/rj4sFNMkk5/p1k2lPUmbm39o4aL7V9XH:10nvE724xoiRQJPrjpLKSFl9oX31Z1d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\RE1Mu3b[1].png	
MD5:	9F14C20150A003D7CE4DE57C298F0FBA
SHA1:	DAA53CF17CC45878A1B153F3C3BF47DC9669D78F
SHA-256:	112FEC798B78AA02E102A724B5CB1990C0F909BC1D8B7B1FA256EAB41BBC0960
SHA-512:	D4F6E49C854E15FE48D6A1F1A03FDA93218AB8FCDB2C443668E7DF478830831ACC2B41DAEFC25ED38FCC8D96C4401377374FED35C36A5017A11E63C8DAE5C87
Malicious:	false
IE Cache URL:	http://https://img-prod-cms-rt-microsoft-com.akamaized.net/cms/api/am/imageFileData/RE1Mu3b?ver=5c31
Preview:	.PNG.....IHDR.....J.....tEXtSoftware.Adobe ImageReadyq.e<...(iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c132 79.159284, 2016/04/19-13:13:40 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:DocumentID="xmp.did:A00BC639840A11E68CBEB97C2156C7FD" xmpMM:InstanceID="xmp.iid:A00BC638840A11E68CBEB97C2156C7FD" xmp:CreatorTool="Adobe Photoshop CC 2015.5 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:A2C931A470A111E6AEDFA14578553B7B" stRef:documentID="xmp.did:A2C931A570A111E6AEDFA14578553B7B"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>.....DIDATx..\..UU.>.7..3....h.L..& j2...h.@.."........`U.....R"..Dq.&.BJR 1.4`$.200...l.....wg.y.[k/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\converged_ux_v2_RfnRCrmapm3W_OFn994CMA2[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	95459
Entropy (8bit):	5.292153801820765
Encrypted:	false
SSDEEP:	1536:QpHDIqBBw+T6azA/PWrF7qvEAFiQcpmKboBdiyMUWC8ErpH/TVTDrwCGNJZ3yU0P:IBFNyUM
MD5:	45F9D10AB99AA66DD6FCE167F7DE0230
SHA1:	D443993E7ADB3108167BCD94E5D3126A2E3EE7EE
SHA-256:	D72952FC8950D26C08C6BAD73D389C35D0EAF164CB73503183A2966DEFAAD991
SHA-512:	0DBCCCB37A3A249C7DBB948AC756FD332298DD8A742E92DF6A767FD565C925768058C05AF182106F8DA29979C0D23BD3E9ECE9E41C1EA931F4F198CBDCE8B3F
Malicious:	false
IE Cache URL:	http://https://acctcdn.msauth.net/converged_ux_v2_RfnRCrmapm3W_OFn994CMA2.css?v=1
Preview:	/*! Copyright (C) Microsoft Corporation. All rights reserved. *//*!.---------- START OF THIRD PARTY NOTICE ----------..This file based on or incorporates material from the projects listed below (Third Party IP). The original copyright notice and the license under which Microsoft received such Third Party IP, are set forth below. Such licenses and notices are provided for informational purposes only. Microsoft licenses the Third Party IP to you under the licensing terms for the Microsoft product. Microsoft reserves all other rights not expressly granted under this agreement, whether by implication, estoppel or otherwise. ..//----------.twbs-bootstrap-sass (3.3.0).//----------..The MIT License (MIT)..Copyright (c) 2013 Twitter, Inc..Permission is hereby granted, free of charge, to any perso

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 6 icons, 128x128, 16 colors, 72x72, 16 colors
Category:	downloaded
Size (bytes):	17174
Entropy (8bit):	2.9129715116732746
Encrypted:	false
SSDEEP:	24:QSNTmTFxg4lyyyyyyyyyyyyyio7eeeeeeeekzgsLsLsLsLsQZp:nfgyyyyyyyyyyyyynzQQQQQO
MD5:	12E3DAC858061D088023B2BD48E2FA96
SHA1:	E08CE1A144ECEAE0C3C2EA7A9D6FBC5658F24CE5
SHA-256:	90CDAF487716184E4034000935C605D1633926D348116D198F355A98B8C6CD21
SHA-512:	C5030C55A855E7A9E20E22F4C70BF1E0F3C558A9B7D501CFAB6992AC2656AE5E41B050CCAC541EFA55F9603E0D349B247EB4912EE169D44044271789C719CD0
Malicious:	false
IE Cache URL:	http://https://signup.live.com/Resources/images/favicon.ico
Preview:	.....h(..f...HH.....(..00.....h....6.. .....=.....@.....(....A..(.....(.....P..... ...3333333333

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\icons[1].eot	
SHA1:	9B0FE96AF141AB09183F386F65BC627B8C396460
SHA-256:	EF04649D4D068673CF0FA47EF4C45C8BE291E703F4EC5FC0E507F17839120AA2
SHA-512:	B1E0CFB515FF2298799BA54574899D27B1FC043F66CC4E9591C504F88273B98697B99ED25955DB84986B39ED9F51864611833DC88064B14C29ADC020FBF6E295
Malicious:	false
IE Cache URL:	http://https://assets.onestore.ms/cdnfiles/external/oneui/oneui1.16.2/dist/fonts/icons/icons.eot?
Preview:	$.....LP.....G.....i.c.o.n.s.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .1...0.....i.c.o.n.s..... OS/2@.Mn...(...Vcmap.1.....Jglyf.....dhead.9.....6hhea.$.....$hmtx@.....loca". h...L...Bmaxp.3.`..... name.....post{NK..... .....G..._.<.....|.....|..... .T.....D.I...H.D.I.....PfEd.@.....D.....(..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery-1.11.2.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	95931
Entropy (8bit):	5.394232486761965
Encrypted:	false
SSDEEP:	1536:5P1vk7i6GUHdXXeyQazBu+4HhiO2AEeLNFoqqhJ7SerN5sVI6xcBgPv7E+nzms9d:A4Ud4qhJvNPqcB47MfWWca98HrB
MD5:	5790EAD7AD3BA27397AEDFA3D263B867
SHA1:	8130544C215FE5D1EC081D83461BF4A711E74882
SHA-256:	2ECD295D295BEC062CEDEBE177E54B9D6B19FC0A841DC5C178C654C9CCFF09C0
SHA-512:	781ACEDC99DE4CE8D53D9B43A158C645EAB1B23DFDFD6B57B3C442B11ACC4A344E0D5B0067D4B78BB173ABBDED75FB91C410F2B5A58F71D438AA6266D048 98A
Malicious:	false
IE Cache URL:	http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js
Preview:	/*! jQuery v1.11.2 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l="1.11.2",m=function(a,b){return new m.fn.init(a,b)},n=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,o=/^-ms-/,p=/-([\da-z])/gi,q=function(a,b){return b.toUpperCase()};m.fn=m.prototype={jquery:l,constructor:m,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=m.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return m.each(this,a,b)},map:function(a){return this.pushStack(m.map(this,function(b,c){ret

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	96649
Entropy (8bit):	5.297804550899051
Encrypted:	false
SSDEEP:	1536:G+6LPOpumEEni7iU2e25CxgjDb60nkN8h1utK0Dv+9G1LDrjsNyw5yn/dFZ75Tym:xH7pDuVUNB0lmEGWf
MD5:	E55ECB02E7376CD010C764107EBD513F
SHA1:	FA6D184DF01EC535628DC8FAF38211591BAADFC8
SHA-256:	5776881753B95A0ABE5D1F6EFE3ABE7B83A3265EACCD117DD948E523C044600C
SHA-512:	099C665E1CEE8DF9C5D5C340A14170341BD29E0321875FF08E594B750CFDBF2CA8C9B45B584FCA21F87CBE6CD8A170918CECFF8C9796AAFA3D89F0AA97509A BD
Malicious:	false
IE Cache URL:	http://https://acctcdn.msauth.net/jquerypackage_1.10_5V7LAuc3bNAQx2QQfr1RPw2.js?v=1
Preview:	/*!. * jQuery JavaScript Library v1.10.2. * http://jquery.com/. *. * Includes Sizzle.js. * http://sizzlejs.com/. *. * Copyright 2005, 2013 jQuery Foundation, Inc. and other contributors. * Released under the MIT license. * http://jquery.org/license. *. * Date: 2013-07-03T13:48Z. */.!function(e,t){function n(e){var t=e.length,n=ct.type(e);return ct.isWindow(e)?!1:1===e.nodeType&&t?!0:"array"===n||"function"!==n&&(0===t||"number"==typeof t&&t>0&&t-1 in e)}function r(e){var t=kt[e]={};return ct.each(e.match(pt)||[],function(e,n){t[n]=!0}),t}function i(e,n,r,i){if(ct.acceptData(e)){var o,a,s=ct.expando,u=e.nodeType,l=u?ct.cache:e,c=u?e[s]:e[s]&&s;if(c&&l[c]&&(i||l[c].data)||r!==t||"string"!=typeof n){return c||(c=u?e[s]=tt.pop()||ct.guid++:s),l[c]||(l[c]=u?{}:{"toJSON":ct.noop}),("object"==typeof n||"function"==typeof n)&&(i?l[c]=ct.extend(l[c],n):l[c].data=ct.extend(l[c].data,n)),a=l[c],i||(a.data||(a.data={}),a=a.data),r!==t&&(a[ct.camelCase(n)]=r),"string"==typeof n?(o=a[n],null==o&&(o=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\mwfmdl2-v3.54[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 26288, version 0.0
Category:	downloaded
Size (bytes):	26288
Entropy (8bit):	7.984195877171481
Encrypted:	false
SSDEEP:	768:56JqQaQphRbTHiKNF5z/02h5KpJW3pPOA8Y9g/:gdTTH5XKpJWdH1W/
MD5:	D0263DC03BE4C393A90BDA733C57D6DB
SHA1:	8A032B6DEAB53A33234C735133B48518F8643B92
SHA-256:	22B4DF5C33045B645CAFA45B04685F4752E471A2E933BFF5BF14324D87DEEE12
SHA-512:	9511BEF269AE0797ADDF4CD6F2FEC4AD0C4A4E06B3E5BF6138C7678A203022AC4818C7D446D154594504C947DA3061030E82472D2708149C0709B1A070FDD0E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\mwfmdl2-v3.54[1].woff	
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/mwf/_h/v3.54/mwf.app/fonts/mwfmdl2-v3.54.woff
Preview:	wOFF.....f.....D.....OS/2...X...H...`JM.FVDMX.....^.qcmap.....*.9cvt ...4... ...*....fpgm...T.....Y...gasp...D.....glyf...P..U5.....head..]....2...6.. .Chhea..]....$$...hmtx..]....ye'loca..^.....Gmaxp..`.... ... ./..name..`....8....]..Rpost..f..... .Q.wprep..f$.....x...x.c`.Pf.....:....Q.B3_dHc..`e.bdb... .`@..`...../9.|... V...)00...-.Wx...S....._..m.m.m.m.m;e..y.~.....<p..a.0t.&...a.pa.0B.1..F...Q.ha.0F.3.....q.xa.0A.0L.&...I.da.0E.2L....i.ta.0C.1..f...Y.la.0G.3.....y.|a..@X0,.....E.ba.DX2,....e .ra..BX1..V...U.ja..FX3.....u.za..A.0l.6...M.fa.E.2l....m.va..C.1..v...].na..G.3.....}.~a.p@80.....C.a..pD82.....c.q..pB81..N...S.i..pF83.....s.y..pA.0\.....K.e..pE.2\....k.u..pC.1..n...[. m..pG.3.....{.}...@x0<.....G.c...Dx2<....g.s...Bx1..^...W.k...Fx3.....w.{...A.0|.>...O.g...E.2|....o.w...C.1..~..._.o..08.....?..0$.....x...mL.U.....9.x.`[...&BF@X...V.h.Z..h. .....`n....[..U

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\oneds_Xr2D7Nex80v7A-8bxF8jgQ2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	82052
Entropy (8bit):	5.312628857785992
Encrypted:	false
SSDEEP:	768:paVnZVNvlcxbEFWEI3+d8lLCNMnSpjaQ2Z8q2G/b8bSqY4gs8Lh1mAXbQON9fAvC:cuediuNMk1T/qTlAvrQUAluA
MD5:	5EBD83ECD7B1F34BFB03EF1BC45F2381
SHA1:	CD1E0062A04B11EEB36586766BF5144955250E65
SHA-256:	4C57821AA26F21DEEBC39E3C750BC4FE246C430E5E50F4ADD0CFF53943C8C608
SHA-512:	9B56B2F1F301AD65D03514E1EC557830501805CBB81A891A518601898AE4F3C8A4C063D64036C2E8F1E539E5989CB608D535A01552BCADF008B53D1B699E9E88
Malicious:	false
IE Cache URL:	http://https://acctcdn.msauth.net/oneds_Xr2D7Nex80v7A-8bxF8jgQ2.js?v=1
Preview:	/*!.. * 1DS JS SDK Core, 2.3.4.. * Copyright (c) Microsoft and contributors. All rights reserved... * (Microsoft Internal Only).. */..!function(e,n){"object"==typeof expo rts&&"undefined"!=typeof module?n(exports):"function"==typeof define&&define.amd?define(["exports"],n):n(e.oneDS=e.oneDS||{})}(this,function(c){"use strict";var i="functi on",o="object",n="undefined",a="prototype",s="hasOwnProperty";function e(){return typeof globalThis!==n&&globalThis?globalThis:typeof self!==n&&self?self:typeof window!==n&&window?window:typeof global!==n&&global?global:null}function r(e){var n=Object.create;if(n)return n(e);if(null==e)return{};var t=typeof e;if(t!==o&&t!==i)thr ow new TypeError("Object prototype may only be an Object:"+e);function r(){}return r[a]=e,new r}function t(e){for(var n,t=1,r=arguments.length;t<r;t++)for(var i in n=argu ments[t])Object[a][s].call(n,i)&&(e[i]=n[i]);return e}var u=function(e,n){return(u=Object.setPrototypeOf||{__proto__:[]}instanceof Array&&function(e,n){e.__prot

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\privacystatement[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	330955
Entropy (8bit):	4.858892140419446
Encrypted:	false
SSDEEP:	3072:wA698dd87wNHDmdS9v+6WjUiPryCGZN9ruekUIx4z7ZV/BdQZyNdkugyZCqTDHwu:w287yjftCrYNb8yQZyZCSDH+ekA
MD5:	1AC234014F0DEC871387CAEA0E81A6A7
SHA1:	638BBE7030041918E0D6048BBC3B4784FB5AE4D1
SHA-256:	0C250EDD6730A5526388BDFCF839764885D872D3FDF4BD0CD49DCE9B2951F3A3
SHA-512:	1A73EE9F1BB35932B0A903B07A369444A08E02D9C4846BA7D7D46FAA27311A131788C87B083AE857D7D88D5EB8C70A6200181951FD9FCAC9924F99176DA8EAF
Malicious:	false
Preview:	.<!DOCTYPE html ><html xmlns:mscom="http://schemas.microsoft.com/CMSvNext" xmlns:md="http://schemas.microsoft.com/mscom-data" lang="en-us" xmlns="http ://www.w3.org/1999/xhtml"><head><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta charset="utf-8" /><meta name="viewport" content="width=device-width, initial-scale=1.0" /><link rel="shortcut icon" href="https://www.microsoft.com/favicon.ico?v2" /><script type="text/javascript" src="https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js">...../// Third party scripts and code linked to or referenced from this website are licensed to you by the parties that own such code, not by Microsoft. See ASP.NET Ajax CDN Terms of Use - http://www.asp.net/ajaxlibrary/CDN.ashx... </script><script type="text/javascript" language="javascript">/*<![CDATA[*/if($(document).bind("mobileinit",function(){$.mobile.autoInitializePage=!1}),navigator.userAgent.match(/IEMobile\/10\.0/)){var msViewportStyle=document.createElement ("style");msViewpo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\signup[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	229725
Entropy (8bit):	5.285115547705195
Encrypted:	false
SSDEEP:	1536:Okf5Pv25eFzlF70UgGZ2qWlem/ZvppBVkjB15AXcx648tFPiDWUKDtLSDllqrBPS:Pf4RW2Jem/ZvppB8Brxx6/tF3DulcgQy
MD5:	4D6B9B660AAC5917D8CC8740C5D63335
SHA1:	E060EB719AD81C8932D1E4B7B10A13983E465A0C
SHA-256:	6FDA5532108DD86C28695093D32771355446BF9E3B41B7B5451E4EA1D39F6E66
SHA-512:	3C846FCCF852091CA2E431565265A7C547DB24BE6B9356A5516D0AECF9A0E2750F664BAD8B4B5DF737DBB07F393D3D2B2E5C2C561DEC61EC858BD2C1119DB 5D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\signup[1].htm	
Preview:	.. Copyright (C) Microsoft Corporation. All rights reserved. -->....<!DOCTYPE html>..<html lang="en" xml:lang="en" class="m_ul" dir="ltr" style="">.. <head>.. <link rel="preconnect" href="https://acctcdn.msauth.net" crossorigin>..<link rel="preconnect" href="https://acctcdn.msauth.net" crossorigin>..<meta http-equiv="x-dns-prefetch-control" content="on">..<link rel="dns-prefetch" href="//acctcdn.msauth.net">..<link rel="dns-prefetch" href="//acctcdn.msftauth.net">..<link rel="dns-prefetch" href="//acctcdnmsftuswe2.azureedge.net">..<link rel="dns-prefetch" href="//acctcdnvzeuno.azureedge.net">.... <title>Microsoft account</title>.. <meta http-equiv="Content-Type" content="text/html;charset=utf-8"/><meta name="referrer" content="origin"/><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0, minimum-scale=1.0, user-scalable=yes"/><meta name="format-detection" content="telephone=no"/>.. <link rel="shortcut icon" href="https://acctcdn.msau

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\signup[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	233303
Entropy (8bit):	5.32835072678974
Encrypted:	false
SSDEEP:	1536:Okf5Pv25eFzlF70UgGZ2qWlem/ZUp2BmllB35AXcx648tFPiDWUKDtLSDllqrBTS:Pf4RW2Jem/ZUp2B0BJxx6/tF3DulYgQy
MD5:	F8A7A9A005B7F1779446FBC5D2894C9F
SHA1:	61976009B89096D89EECA460DF29FD13B0CFAD56
SHA-256:	B8C105B6D7C7C1FE1F9E3A1B2E520806E0D4974B6B46925A204E468FFE278A6A
SHA-512:	1885E9C1A14D286660EE9D3731AF223236CB03FAC47B99393FC4E06B0895870341B03C7BB9BCC26CE175C8AA81B24E8E3659BB5CE2275A68449EC1FEC49A9FA5
Malicious:	false
Preview:	.. Copyright (C) Microsoft Corporation. All rights reserved. -->....<!DOCTYPE html>..<html lang="en" xml:lang="en" class="m_ul" dir="ltr" style="">.. <head>.. <link rel="preconnect" href="https://acctcdn.msauth.net" crossorigin>..<link rel="preconnect" href="https://acctcdn.msauth.net" crossorigin>..<meta http-equiv="x-dns-prefetch-control" content="on">..<link rel="dns-prefetch" href="//acctcdn.msauth.net">..<link rel="dns-prefetch" href="//acctcdn.msftauth.net">..<link rel="dns-prefetch" href="//acctcdnmsftuswe2.azureedge.net">..<link rel="dns-prefetch" href="//acctcdnvzeuno.azureedge.net">.... <title>Microsoft account</title>.. <meta http-equiv="Content-Type" content="text/html;charset=utf-8"/><meta name="referrer" content="origin"/><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=2.0, minimum-scale=1.0, user-scalable=yes"/><meta name="format-detection" content="telephone=no"/>.. <link rel="shortcut icon" href="https://acctcdn.msau

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\style[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	836
Entropy (8bit):	4.940950417710206
Encrypted:	false
SSDEEP:	24:Cn5ZoK2kNMCJZ4ZVaeao1DphsILHJNM2WXgEXgf0Xgm:u5dxJZ4+BWIIPLQ73/
MD5:	2AC383F4677A1036C8EA4289F99A31E3
SHA1:	E65967B9273029CDDD5A5F8DF9E61DACF89CF11C
SHA-256:	2206A95E6BAC7C185CC54638EBF0B0089CBC27FF729B45AC63C968CFE4991AA4
SHA-512:	9E61D4E2B42A1BC776C5649ECD2E32A1CE1ACEDA929E8C013D20BE95D12B7B56864FD588D6117E6410988331F85E21815E2E135030F49BEA2A244F872570DBE
Malicious:	false
IE Cache URL:	http://https://c.s-microsoft.com/en-us/CMSStyles/style.csx?k=4627136a-bd68-db6e-30c9-37cf96c98eee
Preview:	body .grid,.body-open .grid,.grid h3,.grid .h3,.grid .header-small,.grid strong,.grid .body-tight-2,.grid h1,.grid .h1,.grid .header-large,.grid .caption{font-family:"Segoe UI"}.grid{max-width:1600px !important}.c-uhfh-actions,.c-uhfh-gcontainer-st .all-ms-nav,.glyph-global-nav-button{display:none !important}.shell-header-wrapper,.shell-footer-wrapper,.shell-category-nav,.shell-notification .shell-notification-grid-row{max-width:1180px !important}.PsTitle{font-family:Segoe UI,sans-serif;margin-right:.3em !important;font-size:2em;display:inline-block;vertical-align:top;margin-left:-.02em}.childModule{margin-left:8% !important}.CollectingYourInfoRightNav{display:none}html[dir=rtl] .m-r-md{margin-right:0;margin-left:10px}html[dir=rtl] .m-l-md{margin-left:0;margin-right:10px}html[dir=rtl] .m-r-bl{margin-right:0;margin-left:40px}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ux.converged.login.strings-en.min_yruqtyo0qslo70l4a-_ung2[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	37866
Entropy (8bit):	5.420261274428622
Encrypted:	false
SSDEEP:	768:M211No7yeF1tltkdTKNazDRN2ym+d/PngTeDOb8GYTPRUbx3Tg/anqG3lVQYsO6K:56F1tltkdTKNazDRN2ym+d/PngTeDiuo
MD5:	61152AB723B4AAC94EEF497803EFD436
SHA1:	9DD07DEEA63389C32B6C297EA0385B0329FE8F1D
SHA-256:	FFF0B1C545C2119A2855B9028567640F4145C079EFF9B48DA0DDF66DC8D92F6C
SHA-512:	5FD596F105BF2A4CB3CA213B2B5E6CC59C595C04D8BC751EF3E3DF066B635CC638E687645AE4C8E470399E95457310C8EBB435551D34DEF7838EBDEA1C169CF
Malicious:	false
IE Cache URL:	http://https://aadcdn.msauth.net/ests/2.1/content/cdnbundles/ux.converged.login.strings-en.min_yruqtyo0qslo70l4a-_ung2.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ux.converged.login.strings-en.min_yruqtyo0qslo70l4a-_ung2[1].js	
Preview:	!function(e){function o(n){if(i[n])return i[n].exports;var t=i[n]={exports:{},id:n,loaded:!1};return e[n].call(t.exports,t,t.exports,o),t.loaded=!0,t.exports}var i={};return o.m=e,o.c=i,o.p="",o(0)}([function(e,o,i){i(2);var n=i(1),t=i(5),r=i(7),a=r.StringsVariantId,s=r.AllowedIdentitiesType;n.registerSource("str",function(e,o){if(e.WF_STR_SignupLink_AriaLabel_Text="Create a Microsoft account",e.WF_STR_SignupLink_AriaLabel_Generic_Text="Create a new account",e.CT_STR_CookieBanner_Link_AriaLabel="Learn more about Microsoft's Cookie Policy",e.WF_STR_HeaderDefault_Title=o.iLoginStringsVariantId===a.CombinedSigninSignupV2WelcomeTitle?"Welcome":"Sign in",e.STR_Footer_IcpLicense_Text=".ICP.13015306.-10",o.oAppCobranding&&o.oAppCobranding.friendlyAppName){var i=o.fBreakBrandingSigninString?"to continue to {0}":"Continue to {0}";e.WF_STR_App_Title=t.format(i,o.oAppCobranding.friendlyAppName)}switch(o.oAppCobranding&&o.oAppCobranding.signinDescription&&(e.WF_STR_Default_Desc=o.oAppCobrand

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\2_bc3d32a696895f78c19df6c717586a5d[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1864
Entropy (8bit):	5.222032823730197
Encrypted:	false
SSDEEP:	48:yvswNIBLBpJawmMH44log6gw/MHm7pJroog6gwkMH9Xog6gwdMHdqdyqog7C:ykfXYx+odPcs9B
MD5:	BC3D32A696895F78C19DF6C717586A5D
SHA1:	9191CB156A30A3ED79C44C0A16C95159E8FF689D
SHA-256:	0E88B6FCBB8591EDFD28184FA70A04B6DD3AF8A14367C628EDD7CABA32E58C68
SHA-512:	8D4F38907F3423A86D90575772B292680F7970527D2090FC005F9B096CC81D3F279D59AD76EAFCA30C3D4BBAF2276BBAA753E2A46A149424CF6F1C319DED5A6
Malicious:	false
IE Cache URL:	http://https://aadcdn.msauth.net/shared/1.0/content/images/backgrounds/2_bc3d32a696895f78c19df6c717586a5d.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6z" fill="url(#A)"/><path d="M394.2 1815.6c746.58 0 1351.8-493.2 1351.8-1101.6S1140.78-387.6 394.2-387.6-957.6 105.603-957.6 714-352.38 1815.6 394.2 1815.6z" fill="url(#B)"/><path d="M1548.6 1885.2c631.92 0 1144.2-417.45 1144.2-932.4S2180.52 20.4 1548.6 20.4 404.4 437.85 404.4 952.8s512.276 932.4 1144.2 932.4z" fill="url(#C)"/><path d="M265.8 1215.6c690.246 0 1249.8-455.595 1249.8-1017.6S956.046-819.6 265.8-819.6-984-364.005-984 198-424.445 1215.6 265.8 1215.6z" fill="url(#D)"/></g><defs><radialGradient id="A" cx="0" cy="0" r="1" gradientUnits="userSpaceOnUse" gradientTransform="translate(1466.4 393.6) rotate(90) scale(1401.6 1720.8)"><stop stop-color="#107c10"/><stop offset="1" stop-color="#c4c4c4" stop-opacity="0"/></radialGradient><r

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\b5-6bb6f8[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	168682
Entropy (8bit):	5.043901826900668
Encrypted:	false
SSDEEP:	3072:jzCPZkTP3bDLH0tfRqQ0xtLfj4ZDSIpTt813viY8R1j35Ap7LQZLPPJH7PAbOCxq:jlZACLkeedJ
MD5:	32498183608C049E806B05A773254B29
SHA1:	D624684F4E69B3591D95668ECE18E20FE4040211
SHA-256:	ABEA64D238E5567C9A33C0CFD0F0E86DB83B705CBCA4E20A4417CFD341BA7725
SHA-512:	215F84055AD3FF89C421BDF2EC623C3571C0B7A7E5884F7452874857076661B6092828A9CB7B43CE8587CB869DC298D5B0F48B40A64930208D85C139AFC1E1BB
Malicious:	false
IE Cache URL:	http://https://www.microsoft.com/onerfstatics/marketingsites-eus-prod/west-european/shell/_scrf/css/themes=default.device=uplevel_web_pc/2b-325ea8/58-3fa6b0/d0-f82d75/e9-d022d1/dd-c924b8/d6-669136/8b-18f8a3/b5-6bb6f8?ver=2.0
Preview:	@charset "UTF-8";./*! | Copyright 2017 Microsoft Corporation | This software is based on or incorporates material from the files listed below (collectively, "Third Party Code"). Microsoft is not the original author of the Third Party Code. The original copyright notice and the license under which Microsoft received Third Party Code are set forth below together with the full text of such license. Such notices and license are provided solely for your information. Microsoft, not the third party, licenses this Third Party Code to you under the terms in which you received the Microsoft software or the services, unless Microsoft clearly states that such Microsoft terms do NOT apply for a particular Third Party Code. Unless applicable law gives you more rights, Microsoft reserves all other rights not expressly granted under such agreement(s), whether by implication, estoppel or otherwise.*/./*! normalize.css v3.0.3 | MIT License | github.com/necolas/normalize.css */.body{margin:0}.context-uh

Static File Info

General

File type:	PDF document, version 1.7
Entropy (8bit):	7.854239115388337
TrID:	• Adobe Portable Document Format (5005/1) 100.00%
File name:	JTI NETWORK - Proposal & Quote.pdf
File size:	53198
MD5:	29ea210345937690e329258544c4bec9
SHA1:	e9236798b8010c0e244dd5b60b79e257517a3da8
SHA256:	f6724cc9d5c2d6edcaa0dc50be576216345b6b8c681631a206245cba6865b3a1

General

SHA512:	9657fae617070deeeaa613d58e3075886e2975cdde09ef f7d62f0dcc61d1ca7a78ac59e2a96b2ce63147f409b6598 92c2dfa973d8364215de01dce6eb46de35
SSDEEP:	768:yQIo9b136ceD6kYz/6Xr5qR78OW5YZ/fCCOdVM6 8W6Po/9USBuwLzD1r1NBvHFN3:X6C4UWIfqM6F6O9 xB3hVHFNOgj
File Content Preview:	%PDF-1.7..%.....1 0 obj..<</Type/Catalog/Pages 2 0 R/ Lang(en-GB) /Metadata 18 0 R/ViewerPreferences 19 0 R>>..endobj..2 0 obj..<</Type/Pages/Count 1/Kids[3 0 R] >>..endobj..3 0 obj..<</Type/Page/Parent 2 0 R/Reso urces<</ExtGState<</GS5 5 0 R/GS8 8 0 R>>

File Icon



Icon Hash:	74ecccdcd4ccccf0

Static PDF Info

General

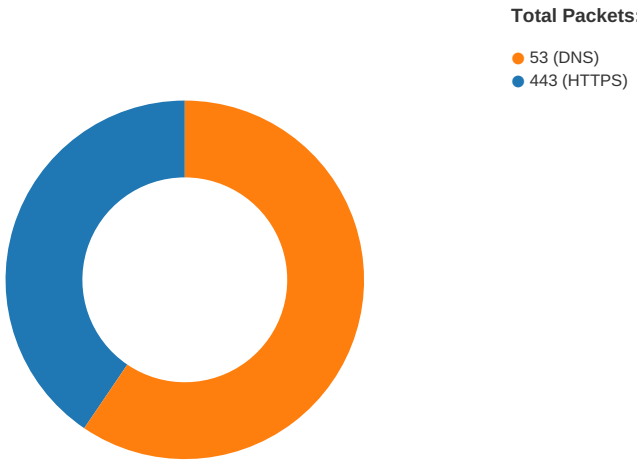
Header:	%PDF-1.7
Total Entropy:	7.854239
Total Bytes:	53198
Stream Entropy:	7.893549
Stream Bytes:	49294
Entropy outside Streams:	5.370544
Bytes outside Streams:	3904
Number of EOF found:	2
Bytes after EOF:	

Keywords Statistics

Name	Count
obj	20
endobj	20
stream	8
endstream	8
xref	2
trailer	2
startxref	2
/Page	1
/Encrypt	0
/ObjStm	0
/URI	4
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Launch	0
/EmbeddedFile	0

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 21:21:34.307784081 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:34.307802916 CET	49735	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:34.507771969 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:34.507988930 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:34.508960962 CET	443	49735	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:34.509201050 CET	49735	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:34.521855116 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:34.521970034 CET	49735	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:34.721697092 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:34.722275972 CET	443	49735	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:34.726741076 CET	443	49735	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:34.726792097 CET	443	49735	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:34.726828098 CET	443	49735	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:34.726906061 CET	49735	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:34.726955891 CET	49735	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:34.728362083 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:34.728401899 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:34.728431940 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:34.728501081 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:34.728563070 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:34.728570938 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:34.758265018 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:34.758377075 CET	49735	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:34.764090061 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:34.960256100 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:34.960339069 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:34.960376978 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:34.960431099 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:34.962201118 CET	443	49735	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:34.962224007 CET	443	49735	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:34.962460995 CET	49735	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.005845070 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.156102896 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.156131983 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.156155109 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.156177044 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.156198978 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.156220913 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.156249046 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.156256914 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.156276941 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.156301022 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.156306982 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.156330109 CET	443	49734	104.153.233.177	192.168.2.3

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 21:21:35.156356096 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.156363010 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.156440973 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.160140038 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.160166979 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.160188913 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.160201073 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.160212994 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.160218000 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.160253048 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.160275936 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.356245041 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.356332064 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.356376886 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.356405973 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.356412888 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.356451035 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.356453896 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.356457949 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.356462955 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.356492996 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.356509924 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.356542110 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.356545925 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.356587887 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.356607914 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.356628895 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.356645107 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.356667995 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.356690884 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.356708050 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.356728077 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.356749058 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.356764078 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.356787920 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.356805086 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.356828928 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.356846094 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.356877089 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.356893063 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.356920004 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.356929064 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.356959105 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.356972933 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.356998920 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.357012987 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.357038021 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.357053041 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.357095003 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.357114077 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.357134104 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.357148886 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.357175112 CET	443	49734	104.153.233.177	192.168.2.3
Feb 22, 2021 21:21:35.357194901 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.357227087 CET	49734	443	192.168.2.3	104.153.233.177
Feb 22, 2021 21:21:35.360075951 CET	443	49734	104.153.233.177	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 21:20:20.567930937 CET	64938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:20.620162010 CET	53	64938	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:21.043037891 CET	60152	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:21.095994949 CET	53	60152	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 21:20:21.841921091 CET	57544	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:21.891932011 CET	53	57544	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:22.776689053 CET	55984	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:22.828432083 CET	53	55984	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:23.535592079 CET	64185	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:23.587023020 CET	53	64185	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:24.560785055 CET	65110	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:24.612566948 CET	53	65110	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:25.920828104 CET	58361	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:25.969759941 CET	53	58361	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:27.468240976 CET	63492	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:27.518356085 CET	53	63492	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:28.413234949 CET	60831	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:28.462119102 CET	53	60831	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:29.300219059 CET	60100	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:29.349127054 CET	53	60100	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:30.283493042 CET	53195	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:30.332329035 CET	53	53195	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:31.228841066 CET	50141	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:31.286284924 CET	53	50141	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:32.179457903 CET	53023	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:32.228286982 CET	53	53023	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:34.349883080 CET	49563	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:34.401494026 CET	53	49563	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:36.832258940 CET	51352	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:36.883929014 CET	53	51352	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:38.573190928 CET	59349	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:38.623513937 CET	53	59349	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:44.153846025 CET	58823	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:44.154081106 CET	57084	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:44.212619066 CET	53	57084	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:44.212668896 CET	53	58823	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:45.145078897 CET	57084	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:45.162399054 CET	58823	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:45.204087019 CET	53	57084	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:45.221050024 CET	53	58823	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:46.145266056 CET	58823	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:46.145409107 CET	57084	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:46.203879118 CET	53	58823	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:46.205074072 CET	53	57084	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:48.161967993 CET	57084	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:48.162693024 CET	58823	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:48.210869074 CET	53	57084	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:48.221501112 CET	53	58823	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:50.628349066 CET	57568	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:50.677340031 CET	53	57568	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:51.832904100 CET	50540	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:51.881886005 CET	53	50540	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:52.224930048 CET	58823	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:52.224989891 CET	57084	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:52.282526016 CET	53	57084	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:52.286892891 CET	53	58823	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:52.772985935 CET	54366	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:52.821772099 CET	53	54366	8.8.8.8	192.168.2.3
Feb 22, 2021 21:20:52.821871996 CET	53034	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:20:52.870533943 CET	53	53034	8.8.8.8	192.168.2.3
Feb 22, 2021 21:21:01.284743071 CET	57762	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:21:01.346415043 CET	53	57762	8.8.8.8	192.168.2.3
Feb 22, 2021 21:21:11.926589966 CET	55435	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:21:11.992454052 CET	53	55435	8.8.8.8	192.168.2.3
Feb 22, 2021 21:21:21.050673962 CET	50713	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:21:21.116005898 CET	53	50713	8.8.8.8	192.168.2.3
Feb 22, 2021 21:21:21.124372959 CET	56132	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:21:21.176012039 CET	53	56132	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 21:21:27.537015915 CET	58987	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:21:27.588989019 CET	53	58987	8.8.8.8	192.168.2.3
Feb 22, 2021 21:21:31.976654053 CET	56579	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:21:32.036582947 CET	60633	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:21:32.039187908 CET	53	56579	8.8.8.8	192.168.2.3
Feb 22, 2021 21:21:32.088171959 CET	53	60633	8.8.8.8	192.168.2.3
Feb 22, 2021 21:21:33.705853939 CET	61292	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:21:33.878407001 CET	63619	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:21:34.289444923 CET	53	61292	8.8.8.8	192.168.2.3
Feb 22, 2021 21:21:34.295532942 CET	53	63619	8.8.8.8	192.168.2.3
Feb 22, 2021 21:21:36.601667881 CET	61946	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:21:36.631867886 CET	64910	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:21:36.658932924 CET	53	61946	8.8.8.8	192.168.2.3
Feb 22, 2021 21:21:36.689083099 CET	53	64910	8.8.8.8	192.168.2.3
Feb 22, 2021 21:21:38.850959063 CET	52123	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:21:38.909967899 CET	53	52123	8.8.8.8	192.168.2.3
Feb 22, 2021 21:21:58.847882986 CET	56338	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:21:58.909977913 CET	53	56338	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:01.802140951 CET	59420	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:01.870569944 CET	53	59420	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:01.970381975 CET	58784	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:02.029747963 CET	53	58784	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:02.459779024 CET	63978	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:02.511696100 CET	53	63978	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:02.984884977 CET	58784	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:03.000516891 CET	62938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:03.033653021 CET	53	58784	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:03.049470901 CET	53	62938	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:03.056971073 CET	55708	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:03.139601946 CET	53	55708	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:03.749921083 CET	56803	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:03.823282003 CET	53	56803	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:03.987303019 CET	58784	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:04.007563114 CET	62938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:04.044603109 CET	53	58784	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:04.056257010 CET	53	62938	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:05.009272099 CET	62938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:05.066553116 CET	53	62938	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:05.454169035 CET	57145	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:05.540312052 CET	53	57145	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:06.047197104 CET	58784	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:06.095978022 CET	53	58784	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:06.605834007 CET	55359	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:06.626043081 CET	58306	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:06.663130045 CET	53	55359	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:06.701638937 CET	53	58306	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:07.025051117 CET	62938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:07.081963062 CET	53	62938	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:08.159456015 CET	64124	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:08.231734037 CET	53	64124	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:10.074567080 CET	58784	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:10.125041008 CET	53	58784	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:10.612277031 CET	49361	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:10.673675060 CET	53	49361	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:11.024296045 CET	62938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:11.073704004 CET	53	62938	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:11.164356947 CET	63150	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:11.207245111 CET	53279	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:11.212447882 CET	56881	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:11.233134031 CET	53	63150	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:11.245521069 CET	53642	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:11.248378992 CET	55667	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:11.269846916 CET	53	53279	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:11.271264076 CET	53	56881	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 21:22:11.306576967 CET	53	53642	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:11.313483000 CET	53	55667	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:14.167865038 CET	54833	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:14.230339050 CET	53	54833	8.8.8.8	192.168.2.3
Feb 22, 2021 21:22:14.821033001 CET	62476	53	192.168.2.3	8.8.8.8
Feb 22, 2021 21:22:14.882352114 CET	53	62476	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 21:21:21.050673962 CET	192.168.2.3	8.8.8.8	0xd7af	Standard query (0)	backblazeb2.com	A (IP address)	IN (0x0001)
Feb 22, 2021 21:21:21.124372959 CET	192.168.2.3	8.8.8.8	0x7885	Standard query (0)	f000.backblazeb2.com	A (IP address)	IN (0x0001)
Feb 22, 2021 21:21:32.036582947 CET	192.168.2.3	8.8.8.8	0x557b	Standard query (0)	f000.backblazeb2.com	A (IP address)	IN (0x0001)
Feb 22, 2021 21:21:33.705853939 CET	192.168.2.3	8.8.8.8	0xb02	Standard query (0)	f000.backblazeb2.com	A (IP address)	IN (0x0001)
Feb 22, 2021 21:21:36.601667881 CET	192.168.2.3	8.8.8.8	0x96f5	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Feb 22, 2021 21:21:58.847882986 CET	192.168.2.3	8.8.8.8	0xb6a0	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Feb 22, 2021 21:22:01.802140951 CET	192.168.2.3	8.8.8.8	0x176d	Standard query (0)	signup.live.com	A (IP address)	IN (0x0001)
Feb 22, 2021 21:22:03.056971073 CET	192.168.2.3	8.8.8.8	0x6916	Standard query (0)	acctcdn.msauth.net	A (IP address)	IN (0x0001)
Feb 22, 2021 21:22:03.749921083 CET	192.168.2.3	8.8.8.8	0x9aa3	Standard query (0)	fpt.live.com	A (IP address)	IN (0x0001)
Feb 22, 2021 21:22:11.212447882 CET	192.168.2.3	8.8.8.8	0x1dea	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Feb 22, 2021 21:22:14.821033001 CET	192.168.2.3	8.8.8.8	0x6e92	Standard query (0)	assets.onestore.ms	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 21:21:21.176012039 CET	8.8.8.8	192.168.2.3	0x7885	No error (0)	f000.backblazeb2.com		104.153.233.177	A (IP address)	IN (0x0001)
Feb 22, 2021 21:21:32.088171959 CET	8.8.8.8	192.168.2.3	0x557b	No error (0)	f000.backblazeb2.com		104.153.233.177	A (IP address)	IN (0x0001)
Feb 22, 2021 21:21:34.289444923 CET	8.8.8.8	192.168.2.3	0xb02	No error (0)	f000.backblazeb2.com		104.153.233.177	A (IP address)	IN (0x0001)
Feb 22, 2021 21:21:36.658932924 CET	8.8.8.8	192.168.2.3	0x96f5	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 21:21:38.909967899 CET	8.8.8.8	192.168.2.3	0xa631	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 21:21:58.909977913 CET	8.8.8.8	192.168.2.3	0xb6a0	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 21:22:01.870569944 CET	8.8.8.8	192.168.2.3	0x176d	No error (0)	signup.live.com	account.msa.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 21:22:01.870569944 CET	8.8.8.8	192.168.2.3	0x176d	No error (0)	account.msa.msidentity.com	account.msa.akadns6.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 21:22:03.139601946 CET	8.8.8.8	192.168.2.3	0x6916	No error (0)	acctcdn.msauth.net	acctcdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 21:22:03.139601946 CET	8.8.8.8	192.168.2.3	0x6916	No error (0)	scdn1efff.wpc.9da5e.alphacdn.net	sni1gl.wpc.alphacdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 21:22:03.139601946 CET	8.8.8.8	192.168.2.3	0x6916	No error (0)	sni1gl.wpc.alphacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Feb 22, 2021 21:22:03.823282003 CET	8.8.8.8	192.168.2.3	0x9aa3	No error (0)	fpt.live.com	fpt.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 21:22:11.271264076 CET	8.8.8.8	192.168.2.3	0x1dea	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 21:22:11.306576967 CET	8.8.8.8	192.168.2.3	0x2177	No error (0)	consentdeliveryfd.azurefd.net	star-azurefd-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 21:22:14.882352114 CET	8.8.8.8	192.168.2.3	0x6e92	No error (0)	assets.onestore.ms	assets.onestore.ms.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

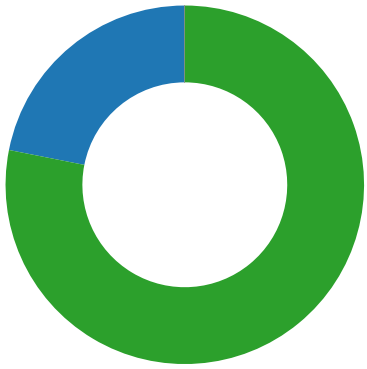
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 22, 2021 21:22:03.239394903 CET	152.199.21.175	443	192.168.2.3	49754	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jan 03 01:00:00 CET 2021 Fri Mar 08 13:00:00 CET 2013	Mon Jan 03 00:59:59 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 22, 2021 21:22:03.239512920 CET	152.199.21.175	443	192.168.2.3	49759	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jan 03 01:00:00 CET 2021 Fri Mar 08 13:00:00 CET 2013	Mon Jan 03 00:59:59 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 22, 2021 21:22:03.239624977 CET	152.199.21.175	443	192.168.2.3	49755	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jan 03 01:00:00 CET 2021 Fri Mar 08 13:00:00 CET 2013	Mon Jan 03 00:59:59 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 22, 2021 21:22:03.239733934 CET	152.199.21.175	443	192.168.2.3	49757	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jan 03 01:00:00 CET 2021 Fri Mar 08 13:00:00 CET 2013	Mon Jan 03 00:59:59 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 22, 2021 21:22:03.239864111 CET	152.199.21.175	443	192.168.2.3	49756	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jan 03 01:00:00 CET 2021 Fri Mar 08 13:00:00 CET 2013	Mon Jan 03 00:59:59 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Feb 22, 2021 21:22:03.240269899 CET	152.199.21.175	443	192.168.2.3	49758	CN=identitycdn.msauth.net, O=Microsoft Corporation, L=Redmond, ST=Washington, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sun Jan 03 01:00:00 CET 2021 Fri Mar 08 13:00:00 CET 2013	Mon Jan 03 00:59:59 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: AcroRd32.exe PID: 404 Parent PID: 5684

General

Start time:	21:20:27
Start date:	22/02/2021
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\JTI NETWORK - Proposal & Quote.pdf'
Imagebase:	0x12b0000
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	object name collision	1	12E65C3	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	object name collision	1	130AE05	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	12FEA85	NtCreateFile
C:\Users\user\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-210223052035Z-195.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	12FEA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5820	write data or add file | append data or add subdirectory or create pipe instance | write ea | read attributes | write attributes | read control | synchronize	device	synchronous io non alert | non directory file	success or wait	1	12FEA85	NtCreateFile
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\acrolock404.1.688666437.tmp	read data or list directory | read ea | read attributes | delete | read control | synchronize	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	1332657	CreateFileW
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	13783C8	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	13783C8	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	13783C8	HttpSendRequestA

Copyright null 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	13783C8	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	13783C8	HttpSendRequestA
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	13783C8	HttpSendRequestA
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R18lzzob_e9dqnf_4ho.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	12FEA85	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	4	12FEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1sc4con_e9dqng_4ho.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	12FEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9Ruddk62_e9dqnh_4ho.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	12FEA85	NtCreateFile
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R1tdmijg_e9dqni_4ho.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	12FEA85	NtCreateFile

Copyright null 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\acrord32_sbx\A9R13v17hf_e9dqnj_4ho.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	12FEA85	NtCreateFile

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeFnt16.lst.5820	C:\Users\user\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt19.lst	success or wait	1	133D405	NtSetInformationFile

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	12FCF19	RegCreateKeyW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0	success or wait	1	12FD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0	success or wait	1	12FD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\SessionManagement\cWindowsCurrent\cWin0\cTab0\cPathInfo	success or wait	1	12FD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\NoTimeOut	success or wait	1	12FD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles	success or wait	1	12BEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	success or wait	1	12BEA55	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	success or wait	1	12BEA55	RegCreateKeyExW
\Device\HarddiskVolume4\Users\user\Desktop\Software\Adobe\Acrobat Reader\DC\TrustManager	success or wait	1	12FD41D	NtCreateKey
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\TrustManager\cDefaultLaunchURLPerms	success or wait	1	12FD41D	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	130DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tDIText	unicode	/C/Users/user/Desktop/JTI NETWORK - Proposal & Quote.pdf	success or wait	1	130DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileName	unicode	JTI NETWORK - Proposal & Quote.pdf	success or wait	1	130DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	tFileSource	unicode	local	success or wait	1	130DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sFileAncestors	binary	5B 5D 00	success or wait	1	130DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDI	binary	2F 43 2F 55 73 65 72 73 2F 68 61 72 64 7A 2F 44 65 73 6B 74 6F 70 2F 4A 54 49 20 4E 45 54 57 4F 52 4B 20 2D 20 50 72 6F 70 6F 73 61 6C 20 26 20 51 75 6F 74 65 2E 70 64 66 00	success or wait	1	130DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	sDate	binary	44 3A 32 30 32 31 30 32 32 32 32 31 32 30 33 34 2D 30 38 27 30 30 27 00	success or wait	1	130DF69	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uFileSize	dword	53198	success or wait	1	130DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c1	uPageCount	dword	1	success or wait	1	130DF89	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	aFS	unicode	CHTTP	success or wait	1	130DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tDIText	unicode	http://www.adobe.com/go/homeacrordrunified18_2018	success or wait	1	130DF47	RegSetValueExW
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	tFileName	unicode	Welcome.pdf	success or wait	1	130DF47	RegSetValueExW

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral\cRecentFiles\c2	sFileAncestors	binary	5B 5D 00	success or wait	1	130DF69	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	130DF69	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 30 32 33 33 34 2D 30 37 27 30 30 27 00	success or wait	1	130DF69	RegSetValueExW

Analysis Process: AcroRd32.exe PID: 5820 Parent PID: 404

General

Start time:	21:20:28
Start date:	22/02/2021
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\JTI NETWORK - Proposal & Quote.pdf'
Imagebase:	0x12b0000
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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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: 6160 Parent PID: 404

General

Start time:	21:20:34
Start date:	22/02/2021
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:	0xb40000

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	success or wait	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\index.html	unknown	4096	end of file	3	C359E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	success or wait	10	C483E5	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	57	success or wait	97	C48447	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	success or wait	218	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main.css	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	success or wait	8	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\init.js	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	success or wait	24	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\plugins.js	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	success or wait	8	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\base_uris.js	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	success or wait	16	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\libs\require\2.1.15\require.min.js	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	success or wait	2176	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\rna-main.js	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	success or wait	60	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef.css	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	success or wait	11	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-ui-theme.css	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	success or wait	8	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\css\main-cef-win.css	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	success or wait	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\config.js	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	success or wait	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\desktop.js	unknown	4096	end of file	4	C359E2	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	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main-selector.css	unknown	4096	end of file	4	C359E2	ReadFile

Copyright null 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	success or wait	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main-selector.css	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\css\main.css	unknown	4096	success or wait	4	C359E2	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	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	success or wait	8	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\css\main.css	unknown	4096	end of file	4	C359E2	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	2	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\plugin-selectors.css	unknown	4096	end of file	2	C359E2	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	3	C359E2	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	3	C359E2	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	3	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\selector.js	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	success or wait	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\selector.js	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	success or wait	24	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files\js\plugin.js	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	success or wait	24	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\my-files-select\js\plugin.js	unknown	4096	end of file	4	C359E2	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	55	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files\js\plugin.js	unknown	4096	end of file	4	C359E2	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	60	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\desktop-connector-files-select\js\plugin.js	unknown	4096	end of file	4	C359E2	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	87	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-selector.js	unknown	4096	end of file	2	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	success or wait	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-selector.css	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	success or wait	55	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\css\main.css	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	success or wait	59	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\css\main.css	unknown	4096	end of file	4	C359E2	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	19	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\css\home-view.css	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	success or wait	20	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\selector.js	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	success or wait	20	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\selector.js	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	success or wait	19	C359E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\selector.js	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	success or wait	240	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\reviews\js\plugin.js	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	success or wait	287	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\signatures\js\plugin.js	unknown	4096	end of file	4	C359E2	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	268	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\tracked-send\js\plugins\tracked-send\js\home-view\plugin.js	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	success or wait	50	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\css\main.css	unknown	4096	end of file	2	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	success or wait	195	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\js\plugins\rhp\exportpdf-rna-tool-view.js	unknown	4096	end of file	2	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	success or wait	32	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\core_icons.png	unknown	4096	end of file	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	success or wait	2	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\aicuc\images\rhp_world_icon.png	unknown	4096	end of file	2	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	success or wait	9	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\images\spectrum_spinner.svg	unknown	4096	end of file	3	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	success or wait	2	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\css\main.css	unknown	4096	end of file	2	C359E2	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	6	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	success or wait	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\selector.js	unknown	4096	end of file	2	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\selector.js	unknown	4096	success or wait	2	C359E2	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	2	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\sign-services-auth\js\selector.js	unknown	4096	success or wait	2	C359E2	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	2	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	success or wait	8	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\home\js\plugin.js	unknown	4096	end of file	2	C359E2	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\uss-search\js\plugin.js	unknown	4096	success or wait	170	C359E2	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	2	C359E2	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	8	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\app-center\css\main-selector.css	unknown	4096	success or wait	1	C359E2	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	2	C359E2	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	16	C359E2	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	2	C359E2	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	C359E2	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	C359E2	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	324	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\add-account\js\selector.js	unknown	4096	success or wait	2	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	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	4	C359E2	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	2	C359E2	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	150	C359E2	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	2	C359E2	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	12	C359E2	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-computer\js\plugin.js	unknown	4096	end of file	2	C359E2	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	32	C359E2	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	2	C359E2	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	10	C359E2	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	2	C359E2	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	2	C359E2	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	2	C359E2	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	4	C359E2	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	2	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css	unknown	4096	success or wait	1	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main-selector.css	unknown	4096	end of file	1	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	success or wait	4	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\css\main.css	unknown	4096	end of file	1	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js	unknown	4096	success or wait	1	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\selector.js	unknown	4096	end of file	1	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js	unknown	4096	success or wait	24	C359E2	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\WebResources\Resource0\static\js\plugins\walk-through\js\plugin.js	unknown	4096	end of file	1	C359E2	ReadFile
\Device\NamedPipe\com.adobe.reader.rna.user.DC.0	unknown	4	pipe broken	1	C483E5	ReadFile

Analysis Process: RdrCEF.exe PID: 6324 Parent PID: 6160

General

Start time:	21:20:36
Start date:	22/02/2021
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=1704,7748200756205629781,9837122587400820282,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=208034491646861541 --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=208034491646861541 --renderer-client-id=2 --mojo-platform-channel-handle=1712 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xb40000
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: 6352 Parent PID: 6160

General

Start time:	21:20:38
Start date:	22/02/2021
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=1704,7748200756205629781,9837122587400820282,131072 --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=KAAAAAAAAACAAwABAQAAAAAAAAAAAGAAAAAAAAAEAAAAIAAAAAAAAACgAAAAEAAAAIAAAAAAAAAAoAAAAAAAAADAAAAAAAAAAAOAAAAAAAAAAQAAAAAAAAAAAAAAAFAAAAEAAAAAAAAAAAAAAABgAAABAAAAAAAAAAAQAAAAUAAAAQAAAAAAAAAAEAAAAGAAAA --use-gl=swiftshader-webgl --log-file='C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log' --service-request-channel-token=15924002696545913488 --mojo-platform-channel-handle=1728 --allow-no-sandbox-job --ignored=' --type=renderer ' /prefetch:2
Imagebase:	0xb40000
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: 6400 Parent PID: 6160

General

Start time:	21:20:40
Start date:	22/02/2021
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=1704,7748200756205629781,9837122587400820282,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=965315283223708852 --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=965315283223708852 --renderer-client-id=4 --mojo-platform-channel-handle=1856 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xb40000
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: 6528 Parent PID: 6160

General

Start time:	21:20:43
Start date:	22/02/2021
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=1704,7748200756205629781,9837122587400820282,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=9191971644911134211 --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=9191971644911134211 --renderer-client-id=5 --mojo-platform-channel-handle=1872 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xb40000
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: 6812 Parent PID: 6160

General

Start time:	21:20:46
Start date:	22/02/2021
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=1704,7748200756205629781,9837122587400820282,131072 --disable-features=VizDisplayCompositor --disable-gpu-compositing --service-pipe-token=6515428939137668262 --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=6515428939137668262 --renderer-client-id=6 --mojo-platform-channel-handle=2148 --allow-no-sandbox-job /prefetch:1
Imagebase:	0xb40000
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: iexplore.exe PID: 5480 Parent PID: 404

General

Start time:	21:21:31
Start date:	22/02/2021

Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' https://f000.backblazeb2.com/file/backup-transistor-71db8aa4/index.html
Imagebase:	0x7ff613e90000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	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	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: iexplore.exe PID: 3864 Parent PID: 5480

General

Start time:	21:21:32
Start date:	22/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5480 CREDAT:17410 /prefetch:2
Imagebase:	0xab0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	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

Disassembly

Code Analysis