ID: 1585398
Sample Name:
SecurityScan_Release.exe
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 15:58:27
Date: 07/01/2025
Version: 41.0.0 Charoite

Table of Contents

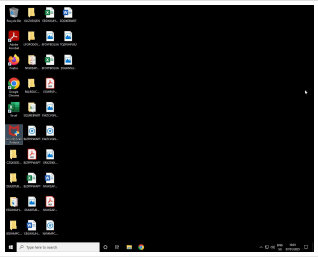
Windows Analysis Report

SecurityScan_Release.exe

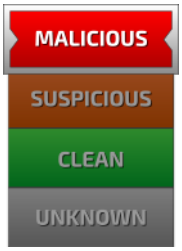
Overview

General Information

Sample name:	SecurityScan_Release.exe
Analysis ID:	1585398
MD5:	d19f7fb266813…
SHA1:	49ad30dc2a86…
SHA256:	9b6d58638033…
Infos:	



Detection

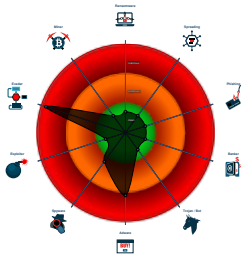


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Checks for kernel code integrity (NtQ…
- Modifies the hosts file
- Queries memory information (via WM…
- Queries sensitive disk information (v…
- Queries sensitive network adapter in…
- Queries sensitive physical memory …
- Queries sensitive service informatio…
- Queries sensitive video device infor…
- Adds / modifies Windows certificates
- Allocates memory with a write watch…
- Checks if Antivirus/Antispyware/Fire…
- Creates a process in suspended mo…

Classification



Process Tree

- **System is w10x64_ra**
- SecurityScan_Release.exe (PID: 3024 cmdline: "C:\Users\user\Desktop\SecurityScan_Release.exe" MD5: D19F7FB266813E0FBA1D009BE48C40D5)
  - MSSPResExtractor.exe (PID: 876 cmdline: "C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\MSSPResExtractor.exe" MD5: 5DC3CCE86B3CEEB218E9F863F2F6138A)
  - mc-webview-cnt.exe (PID: 6492 cmdline: "C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\mc-webview-cnt.exe" McInstallerStartup.dll config:.\Installer.ini mode:/I lang:en-gb MD5: CD7D48BB339C72CCFE7DA3A3164180BC)
    - msedgewebview2.exe (PID: 5868 cmdline: "C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe" --embedded-browser-webview=1 --webview-exe-name=mc-webview-cnt.exe --webview-exe-version=4,2,0,0 --user-data-dir="C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView" --noerrdialogs --embedded-browser-webview-dpi-awareness=2 --enable-features=MojoIpcz --mojo-named-platform-channel-pipe=6492.4264.5447351167827348215 MD5: 9909D978B39FB7369F511D8506C17CA0)
      - msedgewebview2.exe (PID: 980 cmdline: "C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe" --type=crashpad-handler --user-data-dir=C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler --database=C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Crashpad --annotation=IsOfficialBuild=1 --annotation=channel= --annotation=chromium-version=117.0.5938.132 "--annotation=exe=C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe" --annotation=plat=Win64 "--annotation=prod=Edge WebView2" --annotation=ver=117.0.2045.47 --initial-client-data=0x15c,0x160,0x164,0x138,0x170,0x7fff27ef8e88,0x7fff27ef8e98,0x7fff27ef8ea8 MD5: 9909D978B39FB7369F511D8506C17CA0)
      - msedgewebview2.exe (PID: 6204 cmdline: "C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe" --type=gpu-process --noerrdialogs --user-data-dir="C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView" --webview-exe-name=mc-webview-cnt.exe --webview-exe-version=4,2,0,0 --embedded-browser-webview=1 --embedded-browser-webview-dpi-awareness=2 --gpu-preferences=WAAAAAAAAADgAAAMAAAAAAAAAAAAAAAAAABgAAAAAAA4AAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAYAAAAAAAAAAgAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --mojo-platform-channel-handle=1756 --field-trial-handle=1760,i,6605253056815991885,2925413455889371500,262144 --enable-features=MojoIpcz /prefetch:2 MD5: 9909D978B39FB7369F511D8506C17CA0)
      - msedgewebview2.exe (PID: 6212 cmdline: "C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --noerrdialogs --user-data-dir="C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView" --webview-exe-name=mc-webview-cnt.exe --webview-exe-version=4,2,0,0 --embedded-browser-webview=1 --embedded-browser-webview-dpi-awareness=2 --mojo-platform-channel-handle=1924 --field-trial-handle=1760,i,6605253056815991885,2925413455889371500,262144 --enable-features=MojoIpcz /prefetch:3 MD5: 9909D978B39FB7369F511D8506C17CA0)
      - msedgewebview2.exe (PID: 1448 cmdline: "C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-GB --service-sandbox-type=service --noerrdialogs --user-data-dir="C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView" --webview-exe-name=mc-webview-cnt.exe --webview-exe-version=4,2,0,0 --embedded-browser-webview=1 --embedded-browser-webview-dpi-awareness=2 --mojo-platform-channel-handle=2384 --field-trial-handle=1760,i,6605253056815991885,2925413455889371500,262144 --enable-features=MojoIpcz /prefetch:8 MD5: 9909D978B39FB7369F511D8506C17CA0)
      - msedgewebview2.exe (PID: 6220 cmdline: "C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe" --type=renderer --noerrdialogs --user-data-dir="C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView" --webview-exe-name=mc-webview-cnt.exe --webview-exe-version=4,2,0,0 --embedded-browser-webview=1 --embedded-browser-webview-dpi-awareness=2 --disable-nacl --first-renderer-process --lang=en-GB --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=5 --js-flags="--harmony-weak-refs-with-cleanup-some --expose-gc --ms-user-locale=en_CH" --time-ticks-at-unix-epoch=-1736257074872177 --launch-time-ticks=4883734823 --mojo-platform-channel-handle=3308 --field-trial-handle=1760,i,6605253056815991885,2925413455889371500,262144 --enable-features=MojoIpcz /prefetch:1 MD5: 9909D978B39FB7369F511D8506C17CA0)
      - msedgewebview2.exe (PID: 7568 cmdline: "C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe" --type=renderer --noerrdialogs --user-data-dir="C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView" --webview-exe-name=mc-webview-cnt.exe --webview-exe-version=4,2,0,0 --embedded-browser-webview=1 --embedded-browser-webview-dpi-awareness=2 --disable-nacl --disable-gpu-compositing --lang=en-GB --device-scale-factor=1 --num-ra

ster-threads=2 --enable-main-frame-before-activation --renderer-client-id=6 --js-flags="--harmony-weak-refs-with-cleanup-some --expose-gc --ms-user-locale=en_CH" --time-ticks-at-unix-epoch=-1736257074872177 --launch-time-ticks=4896010912 --mojo-platform-channel-handle=4424 --field-trial-handle=1760,i,660525305681599188 5,2925413455889371500,262144 --enable-features=MojoIpcz /prefetch:1 MD5: 9909D978B39FB7369F511D8506C17CA0)
    - MSSPResExtractor.exe (PID: 852 cmdline: "C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\MSSPResExtractor.exe" MD5: 5DC3CCE86B3CEEB218E9F863F2F6138A)
- SecurityScan_Release.exe (PID: 6988 cmdline: "C:\Users\user\Desktop\SecurityScan_Release.exe" MD5: D19F7FB266813E0FBA1D009BE48C40D5)
- SecurityScan_Release.exe (PID: 7060 cmdline: "C:\Users\user\Desktop\SecurityScan_Release.exe" MD5: D19F7FB266813E0FBA1D009BE48C40D5)
    - MSSPResExtractor.exe (PID: 7412 cmdline: "C:\Users\user\AppData\Local\Temp\nsz6D3B.tmp\MSSPResExtractor.exe" MD5: 5DC3CCE86B3CEEB218E9F863F2F6138A)
    - mc-webview-cnt.exe (PID: 7440 cmdline: "C:\Users\user\AppData\Local\Temp\nsz6D3B.tmp\mc-webview-cnt.exe" McInstallerStartup.dll config:.\Installer.ini mode:/I lang:en-gb MD5: CD7D48BB339C72CCFE7DA3A3164180BC)
        - msedgewebview2.exe (PID: 7520 cmdline: "C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe" --embedded-browser-webview=1 --webview-exe-name=mc-webview-cnt.exe --webview-exe-version=4,2,0,0 --user-data-dir="C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView" --noerrdialogs --embedded-browser-webview-dpi-awareness=2 --enable-features=MojoIpcz --mojo-named-platform-channel-pipe=7440.7516.17558896153089345560 MD5: 9909D978B39FB7369F511D8506C17CA0)
            - msedgewebview2.exe (PID: 7544 cmdline: "C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe" --type=crashpad-handler --user-data-dir=C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler --database=C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Crashpad --annotation=IsOfficialBuild=1 --annotation=channel= --annotation=chromium-version=117.0.5938.132 "--annotation=exe=C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe" --annotation=plat=Win64 "--annotation=prod=Edge WebView2" --annotation=ver=117.0.2045.47 --initial-client-data=0x160,0x164,0x168,0x13c,0x174,0x7fff27ef8e88,0x7fff27ef8e98,0x7fff27ef8ea8 MD5: 9909D978B39FB7369F511D8506C17CA0)
        - MSSPResExtractor.exe (PID: 7644 cmdline: "C:\Users\user\AppData\Local\Temp\nsz6D3B.tmp\MSSPResExtractor.exe" MD5: 5DC3CCE86B3CEEB218E9F863F2F6138A)
        - SecurityScan_Inner.exe (PID: 7864 cmdline: "C:\Users\user\AppData\Local\Temp\nsz6D3B.tmp\\SecurityScan_Inner.exe" /inner MD5: 555332D3D4F3197D171CB5B1331B15D9)
- winver.exe (PID: 2784 cmdline: "C:\Windows\System32\winver.exe" MD5: 63DC2D604B8A96C9962494D1D957DD77)
- **cleanup**

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Suricata Signatures

ET JA3 Hash - Possible Malware - Fake Firefox Font Update

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2025-01-07T15:59:06.997900+0100	2028371	3	Unknown Traffic	192.168.2.16	49712	44.231.153.113	443	TCP
2025-01-07T15:59:06.997900+0100	2028371	3	Unknown Traffic	192.168.2.16	49712	44.231.153.113	443	TCP
2025-01-07T15:59:08.417267+0100	2028371	3	Unknown Traffic	192.168.2.16	49713	44.231.153.113	443	TCP
2025-01-07T15:59:08.417267+0100	2028371	3	Unknown Traffic	192.168.2.16	49713	44.231.153.113	443	TCP
2025-01-07T15:59:19.142014+0100	2028371	3	Unknown Traffic	192.168.2.16	49719	44.231.153.113	443	TCP
2025-01-07T15:59:19.142014+0100	2028371	3	Unknown Traffic	192.168.2.16	49719	44.231.153.113	443	TCP
2025-01-07T16:00:51.862507+0100	2028371	3	Unknown Traffic	192.168.2.16	49890	52.35.229.208	443	TCP
2025-01-07T16:00:51.862507+0100	2028371	3	Unknown Traffic	192.168.2.16	49890	52.35.229.208	443	TCP
2025-01-07T16:01:07.727197+0100	2028371	3	Unknown Traffic	192.168.2.16	49893	52.35.171.66	443	TCP

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2025-01-07T16:01:07.727197+0100	2028371	3	Unknown Traffic	192.168.2.16	49893	52.35.171.66	443	TCP
2025-01-07T16:01:08.787150+0100	2028371	3	Unknown Traffic	192.168.2.16	49894	52.35.171.66	443	TCP
2025-01-07T16:01:08.787150+0100	2028371	3	Unknown Traffic	192.168.2.16	49894	52.35.171.66	443	TCP

Joe Sandbox Signatures

Spam, unwanted Advertisements and Ransom Demands

Modifies the hosts file

Malware Analysis System Evasion

Queries memory information (via WMI often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive physical memory information (via WMI, Win32_PhysicalMemory, often done to detect virtual machines)

Queries sensitive service information (via WMI, Win32_LogicalDisk, often done to detect sandboxes)

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Anti Debugging

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion

Modifies the hosts file

Lowering of HIPS / PFW / Operating System Security Settings

Modifies the hosts file

Mitre Att&ck Matrix

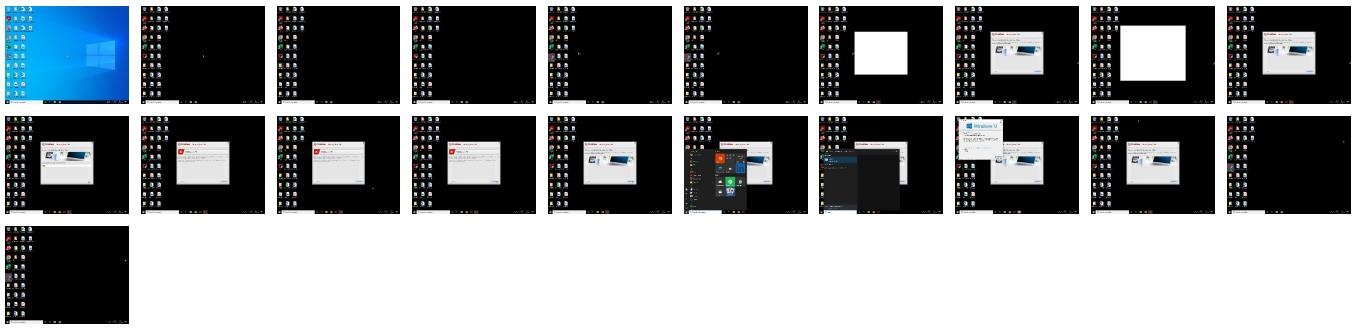
Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	6 3 1 Windows Management Instrumentation	1 DLL Side-Loading	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	Data from Local System	2 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	1 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 File and Directory Permissions Modification	LSASS Memory	7 3 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	1 Non-Application Layer Protocol	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	1 Modify Registry	Security Account Manager	5 4 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	2 Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 Disable or Modify Tools	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Protocol Impersonation	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	5 4 1 Virtualization/Sandbox Evasion	LSA Secrets	2 System Owner/User Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 1 Process Injection	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	1 DLL Side-Loading	DCSync	3 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 3 4 System Information Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement

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
SecurityScan_Release.exe	0%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\InstallHelp\SecurityScanner32.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\McInstallerStartup.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\McUICnt.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\MicrosoftEdgeWebview2Setup.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\SecurityScan_Inner.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\mc-webview-cnt.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\x64\MSSPResExtractor.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\x64\McInstallerRes.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\x64\McInstallerRes_LD.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\x64\McInstallerStartup.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\x64\McUICnt.exe	3%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\x64\McUtil.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\x64\MicrosoftEdgeWebview2Setup.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\x64\SecurityScan_Inner.exe	4%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\x64\WebView2Loader.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\x64\mc-webview-cnt.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsl3F93.tmp\x64\mcbrwsr2.dll	3%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsz6D3B.tmp\MSSPResExtractor.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsz6D3B.tmp\McInstallerRes.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsz6D3B.tmp\McInstallerRes_LD.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsz6D3B.tmp\McUtil.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsz6D3B.tmp\WebView2Loader.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsz6D3B.tmp\mcbrwsr2.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsdF57.tmp\InstallHelp\SecurityScanner32.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

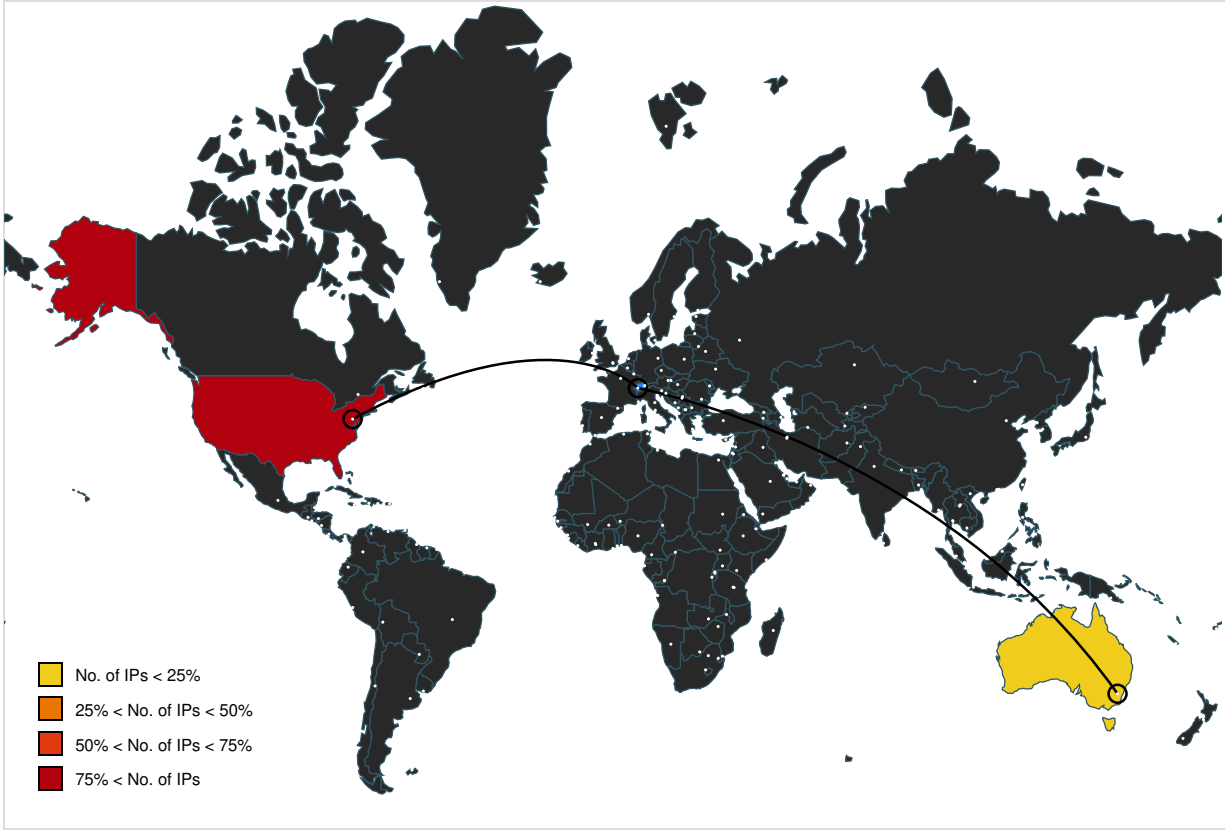
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
chrome.cloudflare-dns.com	162.159.61.3	true	false		high
mosaic-nova.apis.mcafee.com	44.231.153.113	true	false		unknown
analytics.apis.mcafee.com	unknown	unknown	false		unknown
sadownload.mcafee.com	unknown	unknown	false		unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
44.231.153.113	mosaic-nova.apis.mcafee.com	United States		16509	AMAZON-02US	false
162.159.61.3	chrome.cloudflare-dns.com	United States		13335	CLOUDFLARENETUS	false
1.1.1.1	unknown	Australia		13335	CLOUDFLARENETUS	false
13.107.21.239	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.35.229.208	unknown	United States		16509	AMAZON-02US	false
13.107.42.16	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
2.16.168.115	unknown	European Union		20940	AKAMAI-ASN1EU	false
172.64.41.3	unknown	United States		13335	CLOUDFLARENETUS	false
2.16.168.105	unknown	European Union		20940	AKAMAI-ASN1EU	false

General Information

Joe Sandbox version:	41.0.0 Charoite
Analysis ID:	1585398
Start date and time:	2025-01-07 15:58:27 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• EGA enabled

Analysis Mode:	stream
Sample name:	SecurityScan_Release.exe
Detection:	MAL
Classification:	mal72.adwa.evad.winEXE@34/204@17/51
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, svchost.exe
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 2.16.168.115, 2.16.168.105
- Excluded domains from analysis (whitelisted): sadownload.mcafee.com.edgesuite.net, a866.dscd.akamai.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtEnumerateValueKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- Timeout during stream target processing, analysis might miss dynamic analysis data
- VT rate limit hit for: SecurityScan_Release.exe

Created / dropped Files

C:\ProgramData\McAfee Security Scan\ftstate.ini

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	Generic INItialization configuration [DataAnalytics]
Category:	dropped
Size (bytes):	146
Entropy (8bit):	5.192662034541765
Encrypted:	false
SSDEEP:	
MD5:	470CE6E15424116301DDD7F06FA006D0
SHA1:	268C5193F96A1650F17095DB6A73B27571F0B638
SHA-256:	A1F4E1D17703E15A61817278EBFA8AEC0B32300086112F71BB0F2CBBD9BC66E1
SHA-512:	418D2E9C61468367B65594FB80691BE8375EC72E534B146854948207527FB7B0E45C12506AA0240E6D6BF927CE723BC2246788E98BF21710EB4232788FBDD310
Malicious:	false
Reputation:	unknown
Preview:	[queryparams]..affid=0..[DataAnalytics]..InstalledDate=7..InstalledMonth=1..InstalledYear=2025..ProductUUID=8A53D412-9FD3-4039-8B18-BCB7F686E304..

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\aviary_client.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (1531), with CRLF line terminators
Category:	dropped
Size (bytes):	1738
Entropy (8bit):	5.321166453198633
Encrypted:	false
SSDEEP:	
MD5:	1E7EBC68623599ACA8619CC5169F0590
SHA1:	03BED5B7E64E7509B6BA1C5453AF4B553FEACFC5
SHA-256:	8B044EBA3B6C28828C9DCFE6E499BDCBE3EDFC70F4E4C072DB9C050FD48D822F
SHA-512:	79A585371B332CF90FD1686EA53E68509115F6A939E82CCDF4161AFFD3734C828E3223C03FE5636254A89FD38799DC9C4D4D9779FC718A877B548CEEC52BA68
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var aviary_client_fileVersion = "1.4.114"; ..function CreateAviaryClientHelper(){try{var a={Get:function(f){try{if(this._aviaryPlugin){var c=t his._aviaryPlugin.Get(f);this._logInformation("Get: key: "+f+" value:"+JSON.stringify(c));return c}}catch(d){this._logError("Get exception: "+d.message)}return null},Set: function(c,d){if(this._aviaryPlugin){this._aviaryPlugin.Set(c,d)}},ToJsonString:function(){try{if(this._aviaryPlugin){return this._aviaryPlugin.ToJsonString()}}catch(c){t his._logError("ToJsonString exception: "+c.message)}return null},GetDirtyFlag:function(d){try{if(this._aviaryPlugin){return this._aviaryPlugin.GetDirtyFlag(d)}}catch(c){t his._logError("GetDirtyFlag exception: "+c.message)}return true},Setup:function(){try{if(this._aviaryPlugin){return}var f=JSONManager.getSingleton("dictionary");var c=f.d ata;var d=c.product_settings;this._aviaryPlugin=getPluginFactory().Create("ContextItemAviaryStore");this._aviaryPlugin.Initialize(JSON.stringify(d));g

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\common.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe

File Type:	ASCII text, with very long lines (14337), with CRLF line terminators
Category:	dropped
Size (bytes):	14537
Entropy (8bit):	5.3507201842055725
Encrypted:	false
SSDEEP:	
MD5:	BC8BDE16CFD68270180130A481BED8DE
SHA1:	556DAE92A4F6F577C2EB7DC3432EFF23711DB99B
SHA-256:	2A61139B601CB82E007663D7F29F80EDA8616619A03863A42B72F05ED98769A1
SHA-512:	F6853F5DF1EADF477C911D30C20AA4314987DE6F9841C4ABFC8A2FC1836869326B08AB632D9FCFC6B24DCF1E7D21B61D0D0F645F66B7E41DBE96603FBCF045A
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var common_fileVersion = "1.4.114"; ..if(typeof JSON!=="object"){LoadScript("json2.js")}if(typeof enableAnalyticsSDKForUWP==="undefined"){enableAnalyticsSDKForUWP=false}var GetEngineSetting=function(b,a){return a};if(typeof GetSetting==="function"){GetEngineSetting=GetSetting}else{logInformation("Missing GetSetting function; will only use default settings (this is expected pre SDK.2.3)")}var GetEngineProperty=function(b,a){return a};if(typeof GetProperty==="function"){GetEngineProperty=GetProperty}else{logInformation("Missing GetProperty function; will only use default Properties (this is expected pre SDK.2.5)")}if(!enableAnalyticsSDKForUWP){LoadScript("logging.js")}var getSystemPlugin=function(){var a=getScriptVariableStore().Get("system");if(!a){a=getPluginFactory().Create("system");getScriptVariableStore().Set("system",a)}return a};Date.prototype.toISOString=function(a){try{function d(f){var e=String(f);if(e.length===1){e="0"+e}return e}var b=this.getUTCF

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\config_manager.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (842), with CRLF line terminators
Category:	dropped
Size (bytes):	1050
Entropy (8bit):	5.323565161333726
Encrypted:	false
SSDEEP:	
MD5:	5C2EB996C9B5AF003AD9916ADCFE6533
SHA1:	704790B240761930AAB7A541535216FCEBD5C6CD
SHA-256:	46D424408D9487A861CD8BB4900C3610C297B1B9924F2A82AAE0CEC31EBA0E70
SHA-512:	87A0F1B61C1D1F9D2A2D6F53B19487FB6BC88CBA8FB30C4462E22F7F39C7470DDB888D5521F2921669ECA250BD913A46B63F83FB98601B4D3FBA21C7452B11AF
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var config_manager_fileVersion = "1.4.114"; ..function CreateEventConfig(){var a={getEvents:function(){var b=JSONManager.getSingleton("events");return b.data},getProfileNames:function(b){try{return this.getEvents()[b].profileNames}catch(c){return null}},getAttributeRules:function(b){try{return this.getEvents()[b].attributeRules}catch(c){return null}},getPriority:function(c){try{var b=this.getEvents()[c].priority;return b.toLowerCase()}catch(d){return""}},getDataSetNames:function(b){try{return this.getEvents()[b].datasets}catch(c){return[]}},_setEvent:function(d,b){try{return this.getEvents()[d]=b}catch(c){return[]}},getThrottleRule:function(b){try{return this.getEvents()[b].throttleRule}catch(c){logWarning("getThrottleRule: failed, cannot find throttle rule attached to "+b);return null}},_events:null};return a}ModuleManager.registerFactory("config_manager",CreateEventConfig);..//5EE60414C7D07A259D3A495EC0E70D7DD1BC2350CACEDA67835CF4EB5031E387D9398A386B6DD358

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\csp_client.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (3383), with CRLF line terminators
Category:	dropped
Size (bytes):	3587
Entropy (8bit):	5.303660739400768
Encrypted:	false
SSDEEP:	
MD5:	02285FA10F1BFECBB6E0FC79EE757049
SHA1:	64F718E3F85465987B33B6DD29E1C22AF43F79B2
SHA-256:	9B9A6C8721C66C1F29185ECC7F429BBDBB468D63A1273BC12F879830747949A9
SHA-512:	4EED5B2C81D26464D65A1381959CCC8539AED0CBA6A0F0301C696975E6C01899B4221092749778AABE33BA66DAEFBB1DE3E2683B5B59C960864F4844966EBF63
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var csp_client_fileVersion = "1.4.114"; ..function CreateCSPClientHelper(){var a={getClientID:function(c){if(null==c){logError("Invalid (null) appID for CSP::GetClientID");return null}try{var b=this._getPlugin().GetClientID(c);if(!b){this._reportGetClientIDFailure()}return b}catch(d){logError("Failed to retrieve Client ID from CSP for '"+c+"': exception is '"+d.message+"'")}return null},reportEvent:function(b){},getPolicyItem:function(c,b,e){var d="policy_general_settings."+b;if(e){d="policy_general_settings."+e+"."+b}return this._queryPolicyItem(c,d)},getCachedData:function(c,b){try{return this._getPlugin().GetCachedData(c,b)}catch(d){logError("Failed to load cached data for appId='"+c+"', service='"+b+"': exception is '"+d.message+"'")}return null},_getPlugin:function(){if(!this._plugin){this._plugin=getPluginFactory().Create("cspClient");try{var b={policy:"full_sdk_only"};this._plugin.Config(JSON.stringify(b));logNormal("CSP Client plugin configured to us

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\da_definitions.json	
Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	1396
Entropy (8bit):	4.131950546304375
Encrypted:	false
SSDEEP:	
MD5:	6F1D4AE5766E2FC0517756E0E083A679
SHA1:	3763521410A5962C645D0445529EF3997B11CF1D
SHA-256:	DAB0F5582C42B61C79B281A5C358BC7529EF9923793BC869C923DEEFA84708D4
SHA-512:	89F6254BCD0B00EB844D377F4DFF94C7D7946BE294CFA8ED5D2B3CCFFDA6F2ACAC4A062822A7087863B270997D9D6FCC2DCFA952C2664230901D087589C140E
Malicious:	false
Reputation:	unknown
Preview:	{.. "version": "1.4.114",.. "data": {.. "metrics": [.. "event.value",.. "hit.duration.seconds",.. "hit.size.inbytes",.. "hit.engagement.userinitiated",.. "hit.result",.. "hit.metric.1",.. "hit.metric.2",.. "hit.metric.3",.. "hit.metric.4",.. "hit.metric.5",.. "hit.metric.6"..],.. "dimensions": [.. "hit.uniqueid",.. "event.category",.. "event.action",.. "hit.screen",.. "hit.action",.. "hit.engagement.interactive",.. "hit.engagement.desired",.. "sub.category",.. "tertiary.category",.. "guid",.. "hit.session.id",.. "event.label",.. "hit.feature",.. "hit.type",.. "hit.trigger",.. "hit.source",.. "hit.severity",.. "hit.date",.. "hit.label.1",.. "hit.label.2",.. "hit.label.3",.. "hit.label.4",.. "hit.label.5",.. "hit.label.6",.. "hit.label.7",.. "hit.label.8",.. "hit.label.9",.. "hit.labe

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\data_collector.js	
Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (13754), with CRLF line terminators
Category:	dropped
Size (bytes):	13962
Entropy (8bit):	5.21304794720775
Encrypted:	false
SSDEEP:	
MD5:	56D209C4B77DB36DA734EEAF5E666E76
SHA1:	3FF436681EC15CAF7F6724C9DD8E0541FF452CA4
SHA-256:	BBC40E3E1271ADA78E8064F010B53E2DC5BC7C16CFB14A3E7119879B4EBB3E64
SHA-512:	FCD6000DE2E38EBE051BA3C9E8C5CAE8142B348F04FD9423D48C3A213AE89A16F0705F4CA4C1FB0CDAD0D94E08DCC5F3435F9AB4250EA3FCF21109B5513B058A
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var data_collector_fileVersion = "1.4.114"; ..ModuleManager.set("uptime_tracker",function(){return{fetchFromDataDefinition:function(b){try{return null}catch(a){if(a.hasOwnProperty("message")){return"[Plugin method failed: "+a.message+"]"}else{return"[Plugin method failed]"}}}}}());var Create_data_collector=function(){var a={setup:function(){try{this._logInformation("Setup Started.");this._loadDefinitions();this._farmers=this._createFarmers(this);this._refreshers=this._createRefreshers(this);if(!this._farmers||!this._refreshers||!this._definitions){this._logError("Setup failed: farmers("+this._farmers+"). refreshers("+this._refreshers+"). definitions("+this._definitions+")");return}var c=[];for(var b in this._definitions){c.push(b)}this.markDataExpired(c);this._logInformation("Setup Done.")}catch(d){this._logError("Setup failed: "+d.message)}},get:function(h){try{var g=null;if(typeof h==="string"){g=h;h=[h]}if(!h instanceof Array){this._logWarning("get: items

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\data_items.json	
Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	89363
Entropy (8bit):	3.8489514100309172
Encrypted:	false
SSDEEP:	
MD5:	3002F862E16DFADDBA23DC9CC2522523
SHA1:	601654AF4EE33E6E9C1A1DBC1B47C64AC802DE6A
SHA-256:	A6D8DA663A46C45DC8664BAE6A57B8F319BA1CF90676E9E5A63488C329B8C69E
SHA-512:	DB73A811A18A6BDE7983F5E8427E3D2D75D13800EFE220DC2227E0BD6CA401F4DC3147A89FAC36BC4E49DE8251EF3DB5C8F9919EB329DF9EF8B5E26702BAE181
Malicious:	false
Reputation:	unknown
Preview:	{.. "version": "1.4.114",.. "data": {.. "auth0_user_id": {.. "params": "auth0_user_id",.. "source": "settingsManager".. }, .. "user_ref_id": {.. "params": {.. "action": "GetProperty",.. "appid": "vso",.. "name": "user_ref_id".. },.. "refresh": {.. "onMessageBusMsg": [.. "Core.Subscription.Sync",.. "Core.Subscription.SubscriptionUpdated"..].. }, .. "source": "subdb".. },.. "CSP.ClientId": {.. "params": {.. "action": "ClientID",.. "appid": "a053060c-3a34-11e4-8a01-005056b7244f".. },.. "refresh": {.. "harvestIfEqWithTimeout": {.. "value":"[ruleMismatch]",.. "timeout":600000.. },.. "onMessageBusMsg":

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\dataset.js	
Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (7140), with CRLF line terminators
Category:	dropped
Size (bytes):	7341
Entropy (8bit):	5.275074613666029
Encrypted:	false
SSDEEP:	
MD5:	B3E7252726A1A200EE2545087AECE2DA
SHA1:	A21BDEBA3F9DC50707784CA5262C64151B18B6BA
SHA-256:	E73737B43188F5EAF5476502301228DA191E4679FEF2DAD83584C85B3B04A185
SHA-512:	1CF46EDB80E716254FE4458A7C25D8F226A0E2CF3F94980AE10E6F3703F46A4C6A3E8F7C566B0D5A4189A8D87E6D6F9B0F00B9588DB6E412C36324A7A53B9E15
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var dataset_fileVersion = "1.4.114"; ..function CreateDataset(){function b(c){this._name=c;if(!this._name){throw"Dataset created with no name provided"}}b.prototype={initialize:function(d){try{if(!d){this._logError("No configuration defined");return false}var c=d.data_items;if(!c){this._logError("Invalid Data items. Config ("+JSON.stringify(d)+")");return false}this._itemsList=c;var f=d.refresh;this._setRefresh(f);this._logInformation("Initialization complete");return true}catch(g){this._logError("initialize: "+g.message);return false}},get:function(c){try{return this.getContent()[c]}catch(d){this._logError("get: "+d.message)}},getContent:function(){try{this._logInformation("getContent starting");this._logInformation("itemsList"+JSON.stringify(this._itemsList));var d=ModuleManager.getSingleton("data_collector");if(this.dirty){d.markDataExpired(this._itemsList);this.dirty=false}return d.get(this._itemsList)}catch(c){this._logError("getContent: "+c.message)}},

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\dataset_da.js	
Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (6749), with CRLF line terminators
Category:	dropped
Size (bytes):	6953
Entropy (8bit):	5.406921317159456
Encrypted:	false
SSDEEP:	
MD5:	54130B64A7B6C873A442D99B37C94BD2
SHA1:	9997B6D86FEFB276DAF608BFA77A63CBC4A1F8FB
SHA-256:	3386EC5C89C89B296A83F4FB941E12B1BF337782F626F90D0ACE90280995B6A8
SHA-512:	AC3D0E127F5353444638701CFDF4D002B347BE4C0C6A64DAB5D331B306103AE2D7D0B9FC745FD2322ABC6E2C3D2A61F6B4617A75FE2F34D858B6673EE57A72C
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var dataset_da_fileVersion = "1.4.114"; ..var Create_dataset_da=function(){var a={dirty:true,load:function(){if(!this.dirty){return}setTimeout(1*60*60*1000,function(){this.dirty=true});logNormal("Loading dataset da");this._content={};var f=this._getTimeLastDA_Query();if(!f){logInformation("dataset_da: Failed reading query start value. Going to use 0 as start");f=0}var b=this._getTimeNow();if(!b){logError("dataset_da: Failed reading query end value. Going to quit loading the dataset.");return}var c=24*60*60;b=b-c;try{this._processRequests(this._da_queries,f,b);this._store_DA_QueryTime(b)}catch(d){logError("Failed to load the da dataset: exception is '"+d.message+"'");return}this.dirty=false},add:function(b,c){if(!b){return}this._content[b]=c},set:function(b,d,c){if(!c){this.add(b,d);return}var e=ModuleManager.getSingleton("rules");this.add(b,e.apply(d,c))},get:function(b){try{this.load();if(!this._content){return null}return this._content[b]}catch(c){logError

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\datasets_catalog.json	
Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	10553
Entropy (8bit):	4.124349379343266
Encrypted:	false
SSDEEP:	
MD5:	AC18B2AC0D9FC093ACA0D07D01B13218
SHA1:	0C840474541229CC7B64AE19860E3EA85F4DE8A6
SHA-256:	D6D59C37B9F46E3879CAC60239C30A614B3A6AD1B08A9021ABB07D108FC54562
SHA-512:	0FA947D5889ABE619A81960524BFD059F419F0C0EA4A7652A9A6D218BE9BA250FC297D01053F6A43C3445D96B53CE7AEEE93498D40B104D36C9238185CE8CEC7
Malicious:	false
Reputation:	unknown

Preview:	{.. "version": "1.4.114",.. "data": {.. "ab_test":{.. "data_items": [.. "analytics_governance_version",.. "device_id",.. "product_affiliate_id",.. "product_analytics_sdk_version"..],.. "refresh": {.. "useEngineDefaultTimeout": true.. }.. },.. "wss": {.. "data_items": [.. "auth0_user_id",.. "user_ref_id",.. "WSS.Hardware.ID",.. "WSS.Software.ID",.. "WSS.Segment.ID",.. "WSS.Segment.Type.ID",.. "WSS.MSC.Version",.. "WSS.MPF.Version",.. "WSS.MPS.Version",.. "WSS.MQS.Version",.. "WSS.MSK.Version",.. "WSS.NGM.Version",.. "WSS.VUL.Version",.. "WSS.VSO.Version",.. "WSS.VSO.Content.Version",.. "WSS.VSCor

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\dictionary.json

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	20179
Entropy (8bit):	4.552776289770129
Encrypted:	false
SSDEEP:	
MD5:	BC382489643E9DDC228A8D051A42D337
SHA1:	8A99506591E5B90308D02489497361CB5CDEA803
SHA-256:	86F3DDBD547491B25BF67F9BF1A182588EB7DDDB84F3CA875B65B059C1D86896
SHA-512:	CFCE98752EBD973E370880492238B858030A07F27FA2BFA1DAFE619CF37E4B56F6F74D0FFDD93C53551583A8F37570EBB7A1C230ECA0480B48F546882CD9802
Malicious:	false
Reputation:	unknown
Preview:	{.. "version": "1.4.114",.. "data": {.. "event": {},.. "global": {.. "uniqueid": "hit_event_id",.. "uniqueidentifier": "hit_event_id",.. "feature": "hit_feature",.. "trigger": "hit_trigger",.. "interactive": "hit_engagement_interactive",.. "hit.interactive": "hit_engagement_interactive",.. "hit.user.initiated": "hit_engagement_userinitiated",.. "userinitiated": "hit_engagement_userinitiated",.. "desired": "hit_engagement_desired",.. "engagement.desired": "hit_engagement_desired",.. "useridentifier": "hit.userid",.. "label1": "hit_label_1",.. "label2": "hit_label_2",.. "label3": "hit_label_3",.. "label4": "hit_label_4",.. "label5": "hit_label_5",.. "label6": "hit_label_6",.. "metric1": "hit_metric_1",.. "metric2": "hit_metric_2",.. "metric3": "hit_metric_3",.. "metric4": "hit_metric_4",.. "metric5": "hit_metric_5",.. "metric6": "hit_metric_6",.. "screen": "hit_

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\emitter.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (4110), with CRLF line terminators
Category:	dropped
Size (bytes):	4311
Entropy (8bit):	5.214434221619653
Encrypted:	false
SSDEEP:	
MD5:	D8C5553A463C6E0E535E75731984F97E
SHA1:	DC736DD2072CFAC34E33B1BA276B240AEB76239E
SHA-256:	3DDC7CA8246F0B324B2ABBE4750302AB322C92A4AEEEDF3B5AEC3B1712359748
SHA-512:	06F6188B41BD97DB2D7D1981F25DB5C9771BE7ABE650417DD99A3547C90660311E44001864FE452304BA6A5C4F0A90E584F00A637EE6D01587647EFB212B3980
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var emitter_fileVersion = "1.4.114"; ..function createEmitter(b,a){function c(g,i){var h=getScriptVariableStore().Get(g);if(h){return h}try{h=getPluginFactory().Create(i)}catch(j){logError("Failed to create plugin: '"+i+"'")}try{getScriptVariableStore().Set(g,h)}catch(j){logError("Failed to set plugin '"+i+"' in store as '"+g+"'")}return h}try{var d={configure:function(g,e){this.profileName=g;this.profile=e;this.transportName=e.transport;this.transportConfiguration=e.transport_config;this.dataSetNames=e.datasets;this.enableRules=e.enableRules;this.throttleRule=e.throttleRule;this.throttleMultiplier=e.throttleMultiplier;this.maxDimensionLength=e.maxDimensionLength;this.extendedAttributesLengthConfiguration=e.extendedAttributesLength},send:function(h){try{if(!this._isEnabled()){logInformation("_isEnabled() returned false. Will not send data to "+this.transportName);return false}h=this._sanitize(h);if("csp"==this.transportName&&"1"==this._getPlugin(this.transpo

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\engine.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (11329), with CRLF line terminators
Category:	dropped
Size (bytes):	11529
Entropy (8bit):	5.250654475538895
Encrypted:	false
SSDEEP:	
MD5:	BF1603983B0F6F5F4D75FB1206860C8A
SHA1:	D42E9A0DC78B184774227C7D0E86EBB62E904928
SHA-256:	6D01A312285532A3263576F4306D9667411E203DDD3A1A1EF1EAFA7B8FCF4E10
SHA-512:	31873A7F9EE9F466D65B09A565FF505D75657B39A1D96E3AF87DFA88F6378D6FE3FD3333CD73CEACE33AECA1155942B0024AE88AE831E5B1FD09483AAC2DD49C
Malicious:	false
Reputation:	unknown

Preview:	/*! $FileVersion=1.4.114 */ var engine_fileVersion = "1.4.114"; ..LoadScript("common.js");var _factoryManager=CreateFactoryManager();var ModuleManager=CreateModuleManager(_factoryManager);var JSONManager=CreateJSONManager();var StorageManager=CreateStorageManager();var PDManager=CreatePDManager();var RegistryStore=null;var setContentHeartbeatTimeout=function(b,a){var d=getScriptVariableStore().Get("heartbeattimerid");if(d){try{clearInterval(d)}catch(c){logWarning("setContentHeartbeatTimeout: Fail to clear timer id "+c.message)}}d=setTimeout(b,a);getScriptVariableStore().Set("heartbeattimerid",d)};var engine={defaultClientAnalyticsRegistry:GetEngineSetting("Analytics.Base.RegKey","HKLM\\SOFTWARE\\McAfee\\McClientAnalytics"),heartbeatTimestampKey:"analytics_content_heartbeat_timestamp",datasetsRefreshRate:60*60*1000,userId:null,createEventJson:function(c,a){try{a["Tracker.Type"]="event";return{UniqueIdentifier:c,type:"event",payload:a}}catch(b){logError("engine::createEventJson: Exceptio

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\error_transmitter.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (2529), with CRLF line terminators
Category:	dropped
Size (bytes):	2740
Entropy (8bit):	5.312241151375569
Encrypted:	false
SSDEEP:	
MD5:	213154598262F6FB58D03D24B789EBCE
SHA1:	57A9D0906614F8A0A4FFC06303CA7D2014D7DD1F
SHA-256:	9D021EA0C55B0496824431423C36A45A9D37FF293B1EA55B7F54010CC568643C
SHA-512:	C8ECF758190574B5980E60A27D77929925EAF5011FA836861168D7C2F4505DF04FBAC66E018E66F96EAFC9081B1BC592DB8EDF81CAD0EA5EFA1B981A0A510B8
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var error_transmitter_fileVersion = "1.4.114"; ..function CreateAnalyticsErrorTransmitter(){function a(){this.setup()}a.prototype=ModuleManager.create("transmitter_template");a.prototype.messageName="analytics_event_error_occurrred";a.prototype.setup=function(){var c=ModuleManager.getSingleton("config_manager");var d=c.getProfileNames(this.messageName);if(!this.emitter&&d){this.profileName=d[0];this.emitter=this.retrieveEmitter(this.profileName)}};a.prototype._generate=function(c,e){var f={hit_event_id:this.messageName,hit_category_0:"Analytics.Event.Error",hit_trigger:c,hit_action:"Analytics.Event.Rule.Failed"};if(findObjectSize(e.type["ruleMismatch"])){f.hit_category_1="ruleMismatch";f.hit_label_0=JSON.stringify(e)}else{if(findObjectSize(e.type["ruleError"])){f.hit_category_1="ruleError";f.hit_label_0=JSON.stringify(e)}else{if(e.type["rejected"]){f.hit_category_1="rejected";f.hit_label_0=JSON.stringify(e)}}}var d=new Date();f["__record.created"]=d.toISOStr

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\event_handler.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (6709), with CRLF line terminators
Category:	dropped
Size (bytes):	6916
Entropy (8bit):	5.332274302455534
Encrypted:	false
SSDEEP:	
MD5:	92E85B12506AA4D5565097C3061178A4
SHA1:	E7E9704B229B6E1F149CB3F2BACD5C09C4C07686
SHA-256:	2E9F27AB73C48D04F1913723050E8573D3A17A1CF95D842D29CD41E6602A2DFA
SHA-512:	4D6AC930DE75CF9C51A556D14C97CDE438D9C07DE01903CA0C581D7002012563F3AA8BCC8333BA1EEF3C7E372CABE5E7698EBCCB329B9C34BAAA80D43E36FFB
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var event_handler_fileVersion = "1.4.114"; ..if(typeof dataManipulator!=="object"){LoadScript("common.js")}function CreateEventHandler(){var c={handleEvent:function(g){try{var h=JSON.parse(g);var f=h.type;if(("MessageBusPlugin"==f)||("InProcAPI Plugin"==f)){this._processMsgBusEvent(h.payload)}else{if("UWP_Event"==f){this._processAnalyticsAddRecord_v1(h)}else{logWarning("Unexpected message was rejected (unknown type): "+g)}}}catch(i){logError("Failed to process incoming event: exception = '"+i.message+"'")}},handleV1Record:function(e){this._processAnalyticsAddRecord_v1(e)},_processMsgBusEvent:function(h){try{var f=h.name;var k=h.payload;if(("Analytics.v1.AddRecord"==f)||("Analytics.AddRecord"==f)||("Analytics.Automation.AddRecord"==f)){return this._processAnalyticsAddRecord_v1(k)}var j=ModuleManager.getSingleton("data_collector");j.notifyMsg(f);var g=ModuleManager.getSingleton("observation_analytics");g.handle(f,k)}catch(i){logError("Failed to process message

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\events.json

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	218852
Entropy (8bit):	3.07966733633794
Encrypted:	false
SSDEEP:	
MD5:	BAA2C7A097685ECFB8FEC75AC61EF4B8
SHA1:	6838FA7D8EFF2E2A9B3DA6909D45D29FB01068AC
SHA-256:	A3548BE86C732BAA9B3F7535AF98D1C010DB0A49B155672A6AE742FB54EBE40C
SHA-512:	7D1FFA13E6FD472C57E29B87CCD7A256B06B22E6C68FA96F55D26BF9F2DD601F0E49487A1EA31BEA20E0E95E621174333380006C04F595DA843BB1898D7594E

Malicious:	false
Reputation:	unknown
Preview:	{.. "data": {.. "mssplus_antitrack_bottomfixnow_btn_clicked": {.. "attributeRules": {.. "hit_action": {.. "meta": "BottomFixNowButtonCl icked",.. "ruleName": "override".. },.. "hit_category_0": {.. "meta": "clicks",.. "ruleName": "override".. } ,.. "hit_label_0": {.. "meta": "Button",.. "ruleName": "override".. },.. "hit_result": {.. "meta": [.. "Green A",.. "Green B",.. "Yellow",.. "Red",.. "Orange",.. "Blue1",.. "Blue2",.. "NotScanned"..],.. "ruleName": "in".. }.. },.. "curren

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\hash128.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (4059), with CRLF line terminators
Category:	dropped
Size (bytes):	4260
Entropy (8bit):	5.611655458668878
Encrypted:	false
SSDEEP:	
MD5:	51F63AE068525A0A9CE65CB747382E5F
SHA1:	AB3B142E93314394CFB1E1D53B8096A9ED43A5C5
SHA-256:	67373CC04DDD025DA7E357B76FC7D469245D182E180468CB837D9693F4D4C58B
SHA-512:	3DC64D39FC387F6DFFC2C9F5A1FC20021C5DD3B0C30C8B91FAE609D91057308CBDF09AAEC4C526B0DC633CE232097082271934C4DE8B6E6581553948259DC3 4
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var hash128_fileVersion = "1.4.114"; ..function CreateHasher128(){var a={hash128:function(s){function L(c,b){return(c<<b)|(c>>>(32-b))}functio n K(x,c){var G,b,k,F,d;k=(x&2147483648);F=(c&2147483648);G=(x&1073741824);b=(c&1073741824);d=(x&1073741823)+(c&1073741823);if(G&b){return(d^2147483648 ^k^F)}if(G|b){if(d&1073741824){return(d^3221225472^k^F)}else{return(d^1073741824^k^F)}}else{return(d^k^F)}}function r(b,d,c){return(b&d)|((~b)&c)}function q(b,d,c) {return(b&c)|(d&(~c))}function p(b,d,c){return(b^d^c)}function n(b,d,c){return(d^(b|(~c)))}function u(G,F,aa,Z,k,H,I){G=K(G,K(K(r(F,aa,Z),k),I));return K(L(G,H),F)}function f(G,F,aa,Z,k,H,I){G=K(G,K(K(q(F,aa,Z),k),I));return K(L(G,H),F)}function D(G,F,aa,Z,k,H,I){G=K(G,K(K(p(F,aa,Z),k),I));return K(L(G,H),F)}function t(G,F,aa,Z,k,H,I){ G=K(G,K(K(n(F,aa,Z),k),I));return K(L(G,H),F)}function e(x){var H;var k=x.length;var d=k+8;var c=(d-(d%64))/64;var G=(c+1)*16;var I=Array(G-1);var b=0;var F=0;w hile(F<k){H=(F-(F%4)

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\json2.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (3618), with CRLF line terminators
Category:	dropped
Size (bytes):	3817
Entropy (8bit):	5.534649553785636
Encrypted:	false
SSDEEP:	
MD5:	6427079324D5008E719994CD57D6F2AB
SHA1:	57A28074280273933F49A51F1E9059FE00E73F8D
SHA-256:	D7201AA522A70C9A39564D271BF9F19F4CC59216D017B88F2EA08B7125DA2A7A
SHA-512:	F5B6689F66C1A23DA1BE805D0873FC52A594F0CB9D31B06B51F7F39E35BEFCC3734E6E96B56E6548B3D00FAD5BE3056BC5F72927766D0D1459F509002121004
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var JSON2_fileVersion = "1.4.114"; ..if(typeof JSON!=="object"){JSON={}}(function(){var rx_one=/^[\],:{}\s]*$/;var rx_two=/\\(?:["\\\/bfnrt]\u[0-9a-fA-F]{4})/g;var rx_three=/"[^"\\\n\r]*"|true|false|null|-?\d+(?:\.\d*)?(?:[eE][+\-]?\d+)?/g;var rx_four=/(?:^|:|,)(?:\s*\[)+/g;var rx_escapable=/[\\"\u0000-\u001f\u007f-\u009f\u00ad\u0600-\u0604\u070f\u17b4\u17b5\u200c-\u200f\u2028-\u202f\u2060-\u206f\ufeff\ufff0-\uffff]/g;var rx_dangerous=/[\u0000\u00ad\u0600-\u0604\u070f\u17b4\u17b5\u200c-\u200f\u2028-\u202f\u2060-\u206f\ufeff\ufff0-\uffff]/g;function f(n){return n<10?"0"+n:n}function this_value(){return this.valueOf()}if(typeof Date.prototype.toJSON!=="function"){Date.prototype.toJSON=function(){return isFinite(this.valueOf())?this.getUTCFullYear()+"-"+f(this.getUTCMonth()+1)+"-"+f(this.getUTCDate())+" T"+f(this.getUTCHours())+":"+f(this.getUTCMinutes())+":"+f(this.getUTCSeconds())+"Z":null};Boolean.prototype.toJSON=this_value;Number.prototype.toJSON=this_valu

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\logging.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (3176), with CRLF line terminators
Category:	dropped
Size (bytes):	3377
Entropy (8bit):	5.47480094679374
Encrypted:	false
SSDEEP:	
MD5:	54E42C81FDCCBE0AC571BA591CD658E8
SHA1:	C0BD91EF58B860F1DA00F16661CB9014E5C4D417
SHA-256:	F064D98CF449EF55F604E1D1EEEE928A010A8C2A06DA3E6EBC0D93E255CEACC4
SHA-512:	7349FF9A2475B991B45A738AC328377B40300401F44F365B86EFF687183F9C954637DD867C0741903D61A4EB44811B71E0E6FAC155CEE75D82731D841FED6866

Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var logging_fileVersion = "1.4.114"; ..var debugEnable=false;function callerName(){var a=arguments.callee.toString();a=a.substr("function ".length);a=a.substr(0,a.indexOf("("));return a}function getLogger(){var b=getScriptVariableStore().Get("logging");if(b){return b}try{b=getPluginFactory().Create("logging");try{debugEnable=GetEngineProperty("Analytics.SDK.Script.Debug.Enable",debugEnable)}catch(a){}}catch(a){b={LogMessage:function(){},WriteToConsole:function(){},WriteToSyslog:function(){}}}getScriptVariableStore().Set("logging",b);return b}var LOG_SEVERITY_NORMAL=1;var LOG_SEVERITY_WARNING=2;var LOG_SEVERITY_INFORMATION=3;var LOG_SEVERITY_ERROR=4;var LOG_SEVERITY_CRITICAL=5;var SYSLOG_EMERG="emerg";var SYSLOG_ALERT="alert";var SYSLOG_CRITICAL="crticial";var SYSLOG_ERROR="error";var SYSLOG_WARN="warn";var SYSLOG_NOTICE="notice";var SYSLOG_INFO="info";var SYSLOG_DEBUG="debug";var logNormal=function(b){try{b=sanitizeLogMessage(b);getLogger().LogMessage(LOG_SE

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\mappings.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (2160), with CRLF line terminators
Category:	dropped
Size (bytes):	2362
Entropy (8bit):	5.338981928348514
Encrypted:	false
SSDEEP:	
MD5:	9B96221B31737995796F892F0DBDB4BA
SHA1:	9F27EF2BFA85A958F099B7B37B03531BECE00C23
SHA-256:	633CBDBBAE59548247F68C69151F2EC96222B429BC05BC43F3517263BAB39284
SHA-512:	9197C76CBD438273FC28ECCEDC48579C5EFB7F5E2FE2384CB81959850EC6B6C5E4261723B3F04504106AD1EBBA72E9DD6126B6DC269A107B898C46BCC072E7EA
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var mappings_fileVersion = "1.4.114"; ..function CreateMapping(){var a={eventMap:function(c,b){if(!(b in this._eventTable)){return c}return this._map(this._eventTable[b],c,true)},globalMap:function(b){return this._map(this._globalTable,b,true)},daMap:function(b){return this._map(this._daTable,b,true)},profileMap:function(c,b){if(!(b in this._profileTable)){return c}return this._map(this._profileTable[b],c,true)},getProfileTableStr:function(b){if(!(b in this._profileTableStr)){return"{}"}else{return this._profileTableStr[b]}},getFlippedProfileTable:function(c){if(!(c in this._profileTable)){logWarning("Requesting flipped table for invalid profile "+c);return{}}if(c in this._flippedProfileTable){return this._flippedProfileTable[c]}this._flippedProfileTable[c]={};for(var b in this._profileTable[c]){var d=this._profileTable[c][b];this._flippedProfileTable[c][d]=b}return this._flippedProfileTable[c]},_map:function(b,f,h){if(!b||!f||(typeof f!=="object")){logWarni

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\mcutil.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (1832), with CRLF line terminators
Category:	dropped
Size (bytes):	2032
Entropy (8bit):	5.421428347091938
Encrypted:	false
SSDEEP:	
MD5:	18378A5EB18C7D41DE0AEA56CB3E2DF3
SHA1:	172EB8905FFB1AA531016074367CDBB2D10EDDCF
SHA-256:	AECEFED3C550360CA15C01458374FF46960FB038DD6CD9E2B674F154C8FDF542
SHA-512:	E9A171B0199E3E78D640BB3F9FBE80E50950901AB7914598B7AF9FD6A6500F061B5965CF4203B791BD2391AACBBC6D192467F95EC69C099474FFFFDF7ECE2690
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var mcutil_fileVersion = "1.4.114"; ..function CreateMcUtilHelper(){var a={_logError:function(b){logError("mcUtil: "+b)},_logInfo:function(b){logInformation("mcUtil: "+b)},_getPlugin:function(){if(!this._plugin){var c=ModuleManager.getSingleton("data_collector");var b=c.get("analytics.sdk.version");if(b.match("^2.[0-5]")){this._logInfo("This SDK does not support mcUtil plugin. sdkVer("+b+")");return null}this._plugin=getPluginFactory().Create("mcUtil")}return this._plugin},_plugin:null,_hardwareId:null,_softwareId:null,storeHardwareAndSoftwareId:function(d){try{this._logInfo("storeHardwareAndSoftwareId - start");if(!this._getPlugin()){return}var b=d;if(!d){var h=ModuleManager.getSingleton("data_collector");var f=h.get("WSS.Hardware.ID");b=(f==="[ruleMismatch]")?true:false;this._logInfo("value: "+f);this._logInfo("storeValue: "+b)}if(!b){this._logInfo("Not going to storeValue");return}this._invokeGetMachineId();if(!this._softwareId){this._logError("storeHardw

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\observability_datasets.json

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	455
Entropy (8bit):	3.582535825574766
Encrypted:	false
SSDEEP:	
MD5:	DC0AF256F66373834F7A5012C4871D13
SHA1:	DBF0432073C2833D23C27007B491028EA887F94F

SHA-256:	2A898C8070B4BCB4100CAD3CE086EC46294EDD9C87694F1D91E6786F78724F72
SHA-512:	766063869D60DB33B7FDFFCD0FC1665DF0203ABEAF8BEE2E25C8C929AA5B1E330AC19F6A97068F9F08CAC3A1304EB28624DE7012AE027666422F7FB6E54EE3F7
Malicious:	false
Reputation:	unknown
Preview:	{.. "version": "1.4.114",.. "data":{.. "Testing.Mock": {.. "map": {.. "Success" : "Received".. },.. "default": {.. "Test.Value" : "Yes".. }.. },.. "analytics_dataset_get": {.. "map": {.. },.. "default": {.. "hit_event_id": "analytics_send_splitio_product_attributes".. }.. }.. }..}....

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\observation_analytics.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (1151), with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2017
Entropy (8bit):	5.263461770158519
Encrypted:	false
SSDEEP:	
MD5:	9A0756A86DD2AEF257CB1467ECAA7BC4
SHA1:	9CCA3D375956F68991E694148E379A0BD1AE28A7
SHA-256:	32B800AE003E25D728A4741777E4F4DB3AFB2D65C7FB79950282CB158C772D34
SHA-512:	A046924B809BA326F7FDA7A981F06BF7900B9C33F49DD298ED0BC90B395518D3BF0577CD165254DF9F657DDCDC5581E4515CBF13A70C06374004E0F6D02C4E8
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var observation_analytics_fileVersion = "1.4.114"; ..function getObservationAnalyticsEngine(){./*. * config format:. * 'Message.Name' : { // name of obsved message on messagebus that we will subscribe to. * 'map' : { // map from message keys --> analytic friendly keys. * 'Count' : 'Metric1', // ex. 'Count' : 123 --> 'Metric1' : 123. * 'Policy' : 'Event.Label' // ex. 'Policy' : 'XYZ' --> 'Event.Label' : 'XYZ'. * },. * 'default' : { // default values that are not specified in the obsved message. * 'hit_event_id' : 'XYZ'. * }. * }. */.var a=function(){var d=JSONManager.getSingleton("observability_datasets");if(!d){d={data:{}}}return d.data};var b=a();var c={start:function(){try{var d=getMessageBus();for(var f in b){d.Subscribe(f)}logDebug("observationEngine Started")}catch(g){logError("observationE

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\operations.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (6532), with CRLF line terminators
Category:	dropped
Size (bytes):	6736
Entropy (8bit):	5.341408996751215
Encrypted:	false
SSDEEP:	
MD5:	6D6033E034A4DC4FF629BB45E34150D1
SHA1:	C82019EAD44792BD22FA045EFBE2FCD338D4D8ED
SHA-256:	63720A1F4C7719ED1ACDEA115494808400A3BAD0BB9C506D79F06960F2CE3A72
SHA-512:	27289FF8D24F4959F682A93052CDB6610B78600D6DBD403CB6699A0C4B919FA612D9FDC26781F9914EC8BE136F424A678D32F4DDBCBE15DC2D4B0141059E6E9
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var operations_fileVersion = "1.4.114"; ..function CreateDataOperations(){var a={apply:function(c,b){try{if(!b){return c}if(!this._isValidValue(c)){this._logWarning("Invalid value Val("+c+"). Operation with operationConfig("+JSON.stringify(b)+") will not be applied");return null}return this[b.name](c,b.params)}catch(d){this._logError("operations:apply: Excption caught("+d.message+". Val("+c+"), operationConfig("+JSON.stringify(b)+")");return null}},noop:function(b){return b},equal:function(b,c){return b==c},isValueValid:function(b){return(b!="[not assigned]")&&(b!="[ruleMismatch]")&&(b!="[ruleError]")},notNull:function(b){return(b!=null)},validLen:function(b){if(!b){return null}try{b=JSON.parse(b)}catch(c){this._logError("validLen: value ("+b+") not an object, exception: "+c.message);b=[]}if(!(b instanceof Array)){this._logWarning("validLen: value not an array ("+b+").");b=[]}return b.length},lenEqual:function(b,c){return(this.validLen(b)==c)},lenGreater:fun

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\preprocessors.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (825), with CRLF line terminators
Category:	dropped
Size (bytes):	1032
Entropy (8bit):	5.403700179750359
Encrypted:	false
SSDEEP:	
MD5:	1957CAD03CE47E5B8B5D52B3540401C1
SHA1:	FEA43BEE58913AE3C613850FBDDA772D2650D52D
SHA-256:	99E222C01573B1CC3CEA085FC065FA7CD1E85A32870CC5D9500888550747A62C

SHA-512:	4302DA56B265DCCD81DF6B3BFC3C52492927DB5654A11F3A1D4F83AC439F357390A72692FFBE11D1C6A55C4E11018F90852C4EEE32A4E2B7AAD08610FA3743 9
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var preprocessors_fileVersion = "1.4.114"; ..function CreatePreprocessors(){var a={noop:function(b){return b},splitByComma:function(b){return b.split(",")},joinWithComma:function(b){return b.join(",")},sum:function(b){var d;for(var c in b){d=b[c]}return d},toInt:function(c){if(typeof(c)=="object"){for(var b in c){logCons ole("toInt value="+c[b]+" parseInt:"+parseInt(c[b]));c[b]=parseInt(c[b])}return c}return parseInt(c)},toString:function(c){if(typeof(c)=="object"){for(var b in c){c[b]=c[b].toStrin g()}return c}return c.toString()},toUpper:function(b){return b.toUpperCase()},apply:function(c,d){logConsole("rules type="+typeof(d)+" rule= "+d+" value="+c+" typeof(valu e)="+typeof(c));if(!d){return c}if(typeof(d)=="object"){for(var b in d){c=this.apply(c,d[b])}return c}return this[d](c)}};return a}ModuleManager.registerFactory("preproce ssors",CreatePreprocessors);..//E20DF6F144E8358CE37E27629DD7FDC5D2F1110A094127B44884C469763A7DEFE90D28FFEAECE05B60E727306E7A6CE2C1

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\profile.json

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	1113
Entropy (8bit):	4.8133512540587
Encrypted:	false
SSDEEP:	
MD5:	CF2FE9FE7C8EB2B706990271E430180D
SHA1:	81C21541C9C504C3A43CB15189E504C04DB97AAD
SHA-256:	E2DD99C69509A5550893DE432A7D75B3C6FA99C4F6D62F40F055E400E5B77356
SHA-512:	39493C928E0361AA4B9B621C9E81BA0CB4D88456E5A9EFCAE7EB5BF200817FB468807C3629635062E8AB288D862A0A460FB99B59AE3A43916BF02791637F2E71
Malicious:	false
Reputation:	unknown
Preview:	{.. "version": "1.4.114",.. "geoInfo": {.. "apikey":"atRBlD3nPU2xVcVHyaHQW9iaT4LUthwd5bgphI4S".. }, .. "data": {.. "profile_ab_test_mosaic_kongapi_100p": {.. "transport": "aws_apigateway_v2",.. "dictionary": "dictionary_abtest_mosaic",.. "datasets": [.. "ab_test"..],.. "appid": "a053060c-3a34-11e4-8a01-005056b7244f",.. "transport_config": {.. "apikey": "eKW5FAM71o3cPLamQdUSc7ITXU0BWGKtWVxISA50",.. "service": "ab-tests",.. "consumer": "core".. },.. "throttleRule": {.. "meta": 250,.. "ruleName": "dailyMax".. }.. },.. "profile_mss_mosaic_kongapi_100p": {.. "transport": "mosaic_api_v2",.. "dictionary": "dictionary_mss_mosaic",.. "datasets": [.. "default",.. "content_metadata",.. "device",.. "wss",.. "mss"..],.. "appid": "458fa1b2-a07f-42a8-a608-4764244bd594",.. "transport_config": {.. "apikey": "htcnZaEGgL9HlF

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\registry.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (2785), with CRLF line terminators
Category:	dropped
Size (bytes):	2987
Entropy (8bit):	5.391906290625516
Encrypted:	false
SSDEEP:	
MD5:	38E8221A1F9954C4581F866D884A24F5
SHA1:	B7C992AE2B74ABDE7408232CEF178EB17AC3C01E
SHA-256:	569D79EE5F8419FB953FD758994F50CC5815D44F4F53DDD5F6EDCE901698EC5B
SHA-512:	05FBAF92671969A9773417A09B4D5B16C5A9EC870589E43B43B3E8CBD82D0837325325F91A8CFC78A97C728000FE960485A0A0DC62CE47E92FCDF970B4607F8
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var registry_fileVersion = "1.4.114"; ..function CreateRegistryHelper(){var a={openKey:function(c,b){if(typeof b=="boolean"){b=false}if(b){lo gDebug("open registry in write mode");return this._getPlugin().CreateReg(c)}logDebug("open registry in read mode");return this._getPlugin().OpenReg(c)},openKey64:function(c,b){if(typeof b=="boolean"){b=false}if(b){logDebug("open registry in write mode (x64)");return this._getPlugin().CreateReg64(c)}logDebug("open registry in read mode (x64)");return this._getPlugin().OpenReg64(c)},queryValue:function(c,b){var g=false;try{if(typeof b==="boolean"){g=b}var f=this._getPlugin().QueryValue(c,g);return f}catch(d){logInformation("Failed to query "+(g?"obfuscated ":"")+"registry key '"+c+"': exception is '"+d.message+"'");return null},setValue:function(d,f,b){var h=false;try{if(typeof b==="boolean"){h=b}var c=this._getPlugin().SetValue(d,f,h);if(!c){logDebug("registry.setvalue failed ("+d+", "+f+")")}return c}catch(g){logInfor

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\rest_transport.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (6423), with CRLF line terminators
Category:	dropped
Size (bytes):	6631
Entropy (8bit):	5.3005420308257545
Encrypted:	false
SSDEEP:	
MD5:	4A7F198BCE36FEB5E08673D1B2D69AA1
SHA1:	FD0862508788BC6D56FF49CF702D146EF1C6F927
SHA-256:	832E54A9AD812A29DC69C8ACE588BCEA85D3B5B655FFD9C12F01AC41FA927D0E

SHA-512:	9DB9E292CB55A337011C2F7E5F84E8681C0830F0E58D8617E1C943E9A2A583CFAEEB132F5F0AAD574CFBDC4EE1C1DC4703B96CDE2AC9DFC2FE5569595AFEE814
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var rest_transport_fileVersion = "1.4.114"; ..function RESTtransportPlugin(){this._plugin=null;this._requestHeaders={};this._url=null;this.RESTClientAvailable=false}RESTtransportPlugin.prototype=ModuleManager.create("transport_template");RESTtransportPlugin.prototype.constructor=RESTtransportPlugin;RESTtransportPlugin.prototype.GetVersion=function(){try{if(!this._plugin){return null}return this._plugin.GetVersion()}catch(a){}};RESTtransportPlugin.prototype._createRESTclientPlugin=function(){try{this._plugin=getPluginFactory().Create("RESTclient");if(!this._plugin){logError("RESTtransportPlugin:: Could not create RESTclient plugin");return false}return true}catch(a){logError("RESTtransportPlugin:: Failed to initialize the plugin for '"+name+"': exception is '"+a.message+"'");return false}};RESTtransportPlugin.prototype._setup=function(){try{this._url=this._config.url;if(!this._url){logError("Invalid (unspecified) URL for '"+this._name+"', version "+this.versi

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\rules.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (3246), with CRLF line terminators
Category:	dropped
Size (bytes):	3445
Entropy (8bit):	5.354970500627735
Encrypted:	false
SSDEEP:	
MD5:	83408E6F5E87F10716813F0609EB9C8B
SHA1:	765C4D09E1988F32E4425F3A1616D2BD49EAE832
SHA-256:	F1877A88D8A1446C8C9C09E8A39F90500DE89F96FC29B8D59FFB07AD579B5A93
SHA-512:	A398E325CDADF4DC3AF8D42292D9CAC4F830650D8064CF3E1280AA74D69AAA792E96A08532C6231A3C5C1624A443B6B99567B712D521DFE33CC1AADCA04AB6D
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var rules_fileVersion = "1.4.114"; ..function CreateRules(){LoadScript("sha256.js");var a={notNull:function(b,c){return(b!=null)},inRange:function(b,c){return(b>=c.min)&&(b<=c.max)},equal:function(b,c){return(b==String(c))},greater:function(b,c){return(b>c)},greaterEqual:function(b,c){return(b>=c)},less:function(b,c){return(b<c)},lessEqual:function(b,c){return(b<=c)},notEqual:function(b,c){return(b!=String(c))},startsWith:function(b,c){return !b.indexOf(c)},endsWith:function(b,c){return b.indexOf(c,b.length-c.length)!==-1},contains:function(b,c){return b.indexOf(c)!==-1},regex:function(c,f){try{var b=new RegExp(f);if(f.expr&&f.flags){b=new RegExp(f.expr,f.flags)}return b.test(c)}catch(d){logWarning("rules.regex exception: "+d.message);return false}},timestamp:function(b,c){if(!b){return false}return(new Date(b).toISOStringms()==b},"in":function(c,d){for(var b in d){if(c==String(d[b])){return true}}return false},isType:function(b,c){return(typeof b===c)},isE

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\sha256.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (709), with CRLF, LF line terminators
Category:	dropped
Size (bytes):	37442
Entropy (8bit):	5.182723724496523
Encrypted:	false
SSDEEP:	
MD5:	30421B29B9EF976CD06AF1C628BDCE00
SHA1:	242FE79E1369C242B8F71F3C16610F1259632F67
SHA-256:	DBC8A47CCB52356B0313A309DB23CD7EED9253846115DC9203735F0883CFB930
SHA-512:	9B13E21E08CA03CDC626CCBE288627251259EB74F66B9B10A7BE30BF45DA17B799E8C752C28DAE39DB996BD2CA2AE01588C8BD7A2358C36D7666B8442AD4F245
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var sha256_fileVersion = "1.4.114"; ../*.Copyright (c) 2008-2017, Brian Turek.All rights reserved...Redistribution and use in source and binary forms, with or without.modification, are permitted provided that the following conditions are met:.. * Redistributions of source code must retain the above copyright notice, this. list of conditions and the following disclaimer.. * Redistributions in binary form must reproduce the above copyright notice,. this list of conditions and the following disclaimer in the documentation. and/or other materials provided with the distribution.. * Neither the name of the the copyright holder nor the names of its. contributors may be used to endorse or promote products derived from this. software without specific prior written permission...THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS".AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE.IMPLIED WARRANTIES OF MERCHANTABI

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\subdb.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (663), with CRLF line terminators
Category:	dropped
Size (bytes):	862
Entropy (8bit):	5.496968261268393
Encrypted:	false
SSDEEP:	
MD5:	944BB4D794B643EB0EA91230EE1DAA3B

SHA1:	3410E315F19B679F15C3CB862490C093A947407F
SHA-256:	432AC632D1C42EE47D994F609AD612B6D19A45275EBA3CFD4B0EA8B8AEB76F6B
SHA-512:	EA65243D1CBC0907C135F95D944B876E3668338E37C9912E5E2F6C6504997A77B0197E090AD292E3B0B4C2AE6FE0C3545FE7786D7F0F778E3A57BF20B770CB8(
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var subdb_fileVersion = "1.4.114"; ..function CreateSubDbHelper(){var a={_getPlugin:function(){if(!this._plugin){this._plugin=getPluginFactory ().Create("subdb")}return this._plugin},_plugin:null,fetchFromDataDefinition:function(c){try{if(!c){logError("subdb:fetchFromDataDefinition: No dataDefinition supplied"); return null}if(c.action==="canIRun"){return this._getPlugin().CanIRun(c.appid)}if(c.action==="GetProperty"){return this._getPlugin().GetProperty(c.appid,c.name)}logError("Unknown action name ("+c.action+")")}catch(b){logError("subdb:fetchFromDataDefinition: "+b.message+". dataDefinition"+JSON.stringify(c))}return null}};return a }ModuleManager.registerFactory("subdb",CreateSubDbHelper);..//5A613539DF54CF27B020D1B04852FE795E7F246B63773C9AB845982A6D7F055C95AA A4EAA30AAAA79E169CF4887FB2ABB0A1137E23886252ADA59378270B96C5++

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\transmitter_template.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (3717), with CRLF line terminators
Category:	dropped
Size (bytes):	3931
Entropy (8bit):	5.349626620456465
Encrypted:	false
SSDEEP:	
MD5:	6F5E954F2F3F060F2ADB4C5767939CE8
SHA1:	CB34ED8B68917BCE7E1BD287E8C7D7E5510D5481
SHA-256:	BE969BD89EFC244C3E758C063C3C38885B96798D3FE24B25AD996B0773CD3561
SHA-512:	2AE07CA3CC09CCB03AA384E8541411860938972F6FA6FA190BDF42399ABA92498D486B5C14261E500FE85BE27047FB7A094D2385CF74B1DD4E4945D8559D280
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var transmitter_template_fileVersion = "1.4.114"; ..function EventTransmitterTemplate(){}EventTransmitterTemplate.prototype={addData SetNames:function(c,d,b){var a=[];if(d.dataSetNames){a=a.concat(d.dataSetNames)}if(b){a=a.concat(b)}a=dataManipulator.arrayRemoveDuplicates(a);logDebug("emitter ProfileName: "+d.profileName+". allDataSetNames: "+JSON.stringify(a));this._mergeDataSets(c,a)},_isEventThrottled:function(b){var c=ModuleManager.getSingleton("config_manager");var a=c.getThrottleRule(b);return this._applyThrottle(b,a)},_isProfileThrottled:function(b,d){var c=ModuleManager.getSingleton("config_manager");var e=c.getPriority(b);if(e!="critical"){var a=this._getProfile(d).throttleRule;return this._applyThrottle(d,a)}return false},_applyThrottle:function(a,c){try{if(!c){return false}var d=ModuleManager.getSingleton("rules");return d.evaluate(a,c)}catch(b){logError("_applyThrottle: "+b.message)}return false},_applyAttributeRules:function(p,o,a){try{var h=Modu

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\transport.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (7089), with CRLF line terminators
Category:	dropped
Size (bytes):	7292
Entropy (8bit):	5.243071797791836
Encrypted:	false
SSDEEP:	
MD5:	DF3D64D883831400BD58879126A95ED9
SHA1:	A7918A06B4801F733712EFD3CCB16ADB68CBC829
SHA-256:	5D19D0E059ADC4ADBB79DDB57380EA066A4A3CA372605C957509948E8730E029
SHA-512:	F598D05B92218DF915968EAE625E10EE1572284BCAA9C80F0F611C7728D5215BE657107F0B5B142B287A42B3485E1B33072086473E5E31174ABDD95783A97E41
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var transport_fileVersion = "1.4.114"; ..function CreateAnalyticsTransport(){function a(){this.retrieveStoredQueue()}a.prototype=ModuleManager .create("transmitter_template");a.prototype.transmit=function(m,s,t,c){logDebug("analyticstransport.transmit message="+JSON.stringify(s)+", profileNames="+JSON. stringify(t)+", datasetNames="+JSON.stringify(c));if(this._isEventThrottled(m)){logDebug("Event "+m+" was event-level throttled");logAutomationError(m,JSON.stri ngify(s),JSON.stringify({level:"info",type:{eventThrottled:m+" is event throttled"}}));return}for(var l in t){try{var o=t[l];if(this._isProfileThrottled(m,o)){logDebug("Event "+m+" was profile-level throttled by "'+o+'"");logAutomationError(m,JSON.stringify(s),JSON.stringify({level:"info",type:{profileThrottled:m+" is profile throttled for "+o}}));continue}i f(engine.isStopRequestReceived()){logWarning("transmitter.prototype.transmit: Stop request received, so stopping all data transmissions..");return}var

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\transport_api_endpoint.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (3250), with CRLF line terminators
Category:	dropped
Size (bytes):	3466
Entropy (8bit):	5.329272530030789
Encrypted:	false
SSDEEP:	
MD5:	F490FF928FA301034C1E5369339D07D6

SHA1:	B1E40CE43DE124FAE928E2BD2102354B1EA31D22
SHA-256:	C67AA9090886CAE34D3522BE5298DFA54BC9BF850845EAB71207BC76F7046D33
SHA-512:	852DA599E669A82D423E5B5DC9A1E358AC84E0E4D502AC4261D6AB721C4FDE8E76C4E4529B6918A5327C5E7DB6694BD50DEF6B5A4D9F665626B45625733592 4
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var transport_api_endpoint_fileVersion = "1.4.114"; ..function CreateAPIEndpointTransport(){function a(){this._url="";this._verb="PUT"}a.proto type=ModuleManager.create("rest_transport");a.prototype.constructor=a;a.prototype._setup=function(){this._url=this._config.url;if(!this._url){logError("APIEndpointTranspo rt:: Initialize failed url not provided");return false}if(this._config.headers){var d=this._config.headers;for(var b in d){this._AddRequestHeader(b,d[b])}}if(this._config.verb){thi s._verb=this._config.verb}this._createRESTclientPlugin();if(this.GetVersion()&&(this.GetVersion()!="1")&&(this.GetVersion()!="2")){this._usingRESTclientPlugin=true;logInf ormation("Calling parent class to setup using the restful plugin");this._plugin.SetHttpMode(this._verb);var c=getSystemPlugin();this._plugin.SetAgentName("McAfee Mosaic API V1 transmitter_"+c.CreateGUID());this._plugin.Connect(this._url)}else{this._plugin=null}return true};a.prototype._sendUsingRestClient=fun

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\transport_aws_apigateway_v1.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (4753), with CRLF line terminators
Category:	dropped
Size (bytes):	4974
Entropy (8bit):	5.407477472670478
Encrypted:	false
SSDEEP:	
MD5:	3A62ECB46D55CE056DDC6B1C82D058B9
SHA1:	EBB67FD4F68661CFD97DEE58D6F2BED9B74F06AC
SHA-256:	BD72241D6717283399EED99DA7F81A6BFB19D2274BE698CB8A3D5BDB5F4EDD2E
SHA-512:	B7959A60CA64C8F3ECFDAFA9D59703351B2DE4844F905C58466AA56CBDA04086B0A4A277CDDCBE8590A4DDDA378C9CAC811950848848742E2E645E76CEFBA 13
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var transport_aws_apigateway_v1_fileVersion = "1.4.114"; ..function CreateAWSAPIGatewayV1Transport(){function b(){this._apikey=null; this._partitionKey=null;this._url="https://{dns}.awscommon.mcafee.com/1.0/{gateway}/v1/record"}b.prototype=ModuleManager.create("rest_transport");b.prototype.co nstructor=b;b.prototype._setup=function(){this._apikey=this._config.apikey;if(!this._apikey){logError("AWS_APIGateway_V1_Transport:: Initialize failed API key not provided");return false}var c=this._config.dns;if(!c){logError("AWS_APIGateway_V1_Transport:: Initialize failed DNS not provided");return false}var e=this._config.gate way;if(!e){logError("AWS_APIGateway_V1_Transport:: Initialize failed Gateway not provided");return false}this._updateURL("{dns}",c);this._updateURL("{gateway}", e);this._partitionKey=engine.getContextId();if(!this._partitionKey){this._partitionKey=generateAlphaNumericString(256)}this._createRESTclientPlugin();if(this.GetVersion() &&(this.GetVersion()

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\transport_da.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (2581), with CRLF line terminators
Category:	dropped
Size (bytes):	2787
Entropy (8bit):	5.38813757973808
Encrypted:	false
SSDEEP:	
MD5:	DAE9DC9F4767E1C1BA0F2292BAF0112B
SHA1:	DB2ED3395B1862ABE2B7F701B9F759609E6CD4D9
SHA-256:	576A92B11C3155A87017BA2E539812286498A8C979F9692C2922708040EB51F1
SHA-512:	CE513638798C7C5CF44D5DFAC6C8ECC238CB94D9C0A5156C7D2F6211B6BF1BE651105A3F69B7349B961823A27EF3B5FAEF8B18D014815FA7017E7EC2D03830 D
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var transport_da_fileVersion = "1.4.114"; ..function CreateDATransport(){var a={Send:function(c){try{var b=this._getMsgBusPlugin();if(!b){logE rror("[DA Transport] Current MsgBus Plugin does not support request/response.");return false}if(!b.IsAvailable()){logWarning("[DA Transport] Message Bus could not be loaded; subscriptions will not be active");return false}var g=ModuleManager.getSingleton("mappings");c=g.daMap(JSON.parse(c));var d=this._ComposePayload(c);if(null==d){return false}b.Publish("Data_Aggregator.Add_Data",d);logDebug("[DA Transport] Emit outbound data: "+d);return true}catch(f){logError("[DA Transport] Exception thrown when sending da event: "+f.message);return false}},_ComposePayload:function(c){try{var b={};var f={};var h={};c["__record.created"]=this._co nvertToLocalDate(new Date()).toISOString();c["__record.created"]=c["__record.created"].split("T").join(" ");for(var d in c){if(this._indexOf(this._metricList,d)!==-1){f[d]=c[d]}if(this._inde

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\transport_eng_observability.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (3274), with CRLF line terminators
Category:	dropped
Size (bytes):	3495
Entropy (8bit):	5.199846052919043

Encrypted:	false
SSDEEP:	
MD5:	93581833279E8522F8EFC14966C3BF04
SHA1:	010DD699BF7509E1B16575EDBD84F559EBE07CC0
SHA-256:	4713BA38325FF8C257CC2F5DB63705AD421137043A5128906B2E5186372844B2
SHA-512:	5C7172048CAB81E0126A3E014DF52FC32300AFB45E5B6A73B3D9CE2E6C657597D201FA22318A508D18084770F4BBD0183738740A2B703E2940F26BE749173B8B
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var transport_eng_observability_fileVersion = "1.4.114"; ..function ObservabilityTransport(){this._transport_api_endpoint_emitter=null;this._url="https://pl8qcwep6c.execute-api.us-west-2.amazonaws.com/prod_v1/v1/record";this._apikey=null;this._verb="PUT";this._partitionKey=null;this.logInfo("New ObservabilityTransport Created")}ObservabilityTransport.prototype=ModuleManager.create("transport_template");ObservabilityTransport.prototype.constructor=ObservabilityTransport;ObservabilityTransport.prototype.logInfo=function(a){logInformation("ObservabilityTransport: "+a)};ObservabilityTransport.prototype.logError=function(a){logError("ObservabilityTransport: "+a)};ObservabilityTransport.prototype.logWarning=function(a){logWarning("ObservabilityTransport: "+a)};ObservabilityTransport.prototype._updateURL=function(a,b){this._url=updateStringWithReplacement(this._url,a,b)};ObservabilityTransport.prototype.GetVersion=function(){try{return engine.getContentVersion()}ca

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\transport_event_hub.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (7985), with CRLF line terminators
Category:	dropped
Size (bytes):	8198
Entropy (8bit):	5.263467139966956
Encrypted:	false
SSDEEP:	
MD5:	656AFACBD15E9B8CA9DBE06F13FEC889
SHA1:	DAD2AB0D6BD92548C1C1C4CA945FD111BFF6B185
SHA-256:	1D8283518587B2EF32DE17049F5F20EC1FCFFE9F15CEE595B3FB8AC9F9949F48
SHA-512:	67D2C75802CE9F4A47DD439B4712ACD9C999D62EB47DD950585174F50C74FEF8BE23AB59E8CC3EB9C24457C4525C27D0475F911953D598AC8D0A0AD1BA050ED
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var transport_event_hub_fileVersion = "1.4.114"; ..function CreateEventHubTransport(){LoadScript("sha256.js");function a(){this._apiVersion=null;this._servicebusNamespace=null;this._eventHubPath=null;this._sharedAccessKey=null;this._sharedAccessName=null;this._sharedAccessToken=null;this._tokenCreationTime=null;this._timeout=60;this._url="https://{servicebusNamespace}.servicebus.windows.net/{eventHubPath}/messages?timeout={timeout}&api-version={apiVersion}"}a.prototype=ModuleManager.create("rest_transport");a.prototype.constructor=a;a.prototype._setup=function(){this._apiVersion=this._config.apiVersion;if(!this._apiVersion){logError("Event_Hub_Transport:: Initialize Invalid (unspecified) _apiVersion");return false}this._servicebusNamespace=this._config.servicebusNamespace;if(!this._servicebusNamespace){logError("Event_Hub_Transport:: Initialize Invalid (unspecified) _servicebusNamespace");return false}this._eventHubPath=this._config.eventHubPath;if(!this._ev

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\transport_ga.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (2200), with CRLF line terminators
Category:	dropped
Size (bytes):	2406
Entropy (8bit):	5.4839496030761605
Encrypted:	false
SSDEEP:	
MD5:	5E5FE66ED895E9253939E2ECF6AFF3D9
SHA1:	407B2A142D0AFFE796A9FBE4267543BEE40FE597
SHA-256:	29E44BD845EA7FE3BDE0EF71C8CF2C334F73DFEE255A54291D4581A200844363
SHA-512:	F1182888702A45F14BF2CDD741489F83BA2CF6B4CAB5B5414017EE41D0C21F2958957098572EE7D39FCA1B5A77C39C6D592D1AE85300703C890491294EB5D9A9
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var transport_ga_fileVersion = "1.4.114"; ..function CreateGATransport(){function a(){}a.prototype=ModuleManager.create("rest_transport");a.prototype.Send=function(c){try{var i=this._ComposePayload(c);if(null==i){return false}var f=this.RESTClientAvailable?this._sendUsingRESTClient(i):this._sendUsingXMLHTTP(i);var d=JSON.parse(c);var h=d.hit_event_id;this._transportLog(h,i,f,this.GetName()+(this.RESTClientAvailable?"_rest":"_xmlhttp"));return f}catch(g){logError("GA_REST_Transport:Send: "+g.message);return false}};a.prototype._sendUsingXMLHTTP=function(f){try{var c=ModuleManager.create("xmlHttpComObj");if(!c.setup()){logError("GA_REST_Transport::_sendUsingXmlHttp: couldnt create a xmlhttpcom");return null}logInformation("GA_REST_Transport::_sendUsingXmlHttp: Using "+c.getSelectedObjName());c.open("POST",this._url,false);c.send(f);var g=c.getResponseHeader("Content-Type");logInformation("contentTypeResp:"+g);return g.match("image/gif")?true:false}catch(d){log

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\transport_mosaic_api_v2.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (4495), with CRLF line terminators
Category:	dropped

Size (bytes):	4712
Entropy (8bit):	5.257620084723445
Encrypted:	false
SSDEEP:	
MD5:	30BB4AFCAAEBFE34DC64A5E227663C1E
SHA1:	38675C1939117C9B1393F2D1804D20819B9B34F8
SHA-256:	A47F219510EC9E1D409CD804BB2C5DF29C02A64AF95ACC0706D123662574A37F
SHA-512:	975914AF2C331B2177AB415D9F95E372DB0F0E477A3BB09C98A088DBE236E5551EBA635C45A7BC3E2ADAACC73805BD076CD125974B45D12B11557DC4631793 7
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var transport_mosaic_api_v2_fileVersion = "1.4.114"; ..function Mosaic_API_V2_Transport(){this._transport_api_endpoint_emitter=null; this._url="apis.mcafee.com/mosaic/2.0/{service}/{consumer}/v1/record";this._apikey=null;this._verb="PUT";this._partitionKey=null;this._service=null;this._consumer=null;th is._environment=null;this._rtHeaders=null;this.logInfo("New Mosaic_API_V2_Transport Created")}Mosaic_API_V2_Transport.prototype=ModuleManager.create(" transport_template");Mosaic_API_V2_Transport.prototype.constructor=Mosaic_API_V2_Transport;Mosaic_API_V2_Transport.prototype.logInfo=function(a){logIn formation("Mosaic_API_V2_Transport: "+a)};Mosaic_API_V2_Transport.prototype.logError=function(a){logError("Mosaic_API_V2_Transport: "+a)};Mosaic_API_V 2_Transport.prototype.logWarning=function(a){logWarning("Mosaic_API_V2_Transport: "+a)};Mosaic_API_V2_Transport.prototype._updateURL=function(a,b){thi s._url=updateStringWithReplacement(this._url,a,b)};Mosaic_API_V2_Trans

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\transport_msgbus.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (3000), with CRLF line terminators
Category:	dropped
Size (bytes):	3210
Entropy (8bit):	5.244849543315333
Encrypted:	false
SSDEEP:	
MD5:	63CD95F661B0AC1FA4092DA021B9D473
SHA1:	3E0B0E70F437880AC4FBB61032EC99D543404EF4
SHA-256:	B5B337CE44977BFDFEE8EF6B114DED28A8BEAFB91AE4576D97AC130FE14E3DB2
SHA-512:	FFA147D95FFB144F2745B1600C67B4B6F15190CF583431CCB8817CB714B4582352F7B7EC9692F88A9317BF37F5CFC6BA9FC688D6050CF3C065A5C400DB93DDC B
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var transport_msgbus_fileVersion = "1.4.114"; ..function MsgBusTransport(){this._msgbus=null;this._msgName=null;this._processorName= null;this._processorConfig=null;this._processors=(function(a){a.logInfo("Creating processors");return{noop:function(c,b){a.logInfo("noop: Returning eventDataObj unmodifie d");return c},simpleMsgComposer:function(c,b){a.logInfo("simpleMsgComposer: Creating new message");var f={};for(var d in b){if(b.hasOwnProperty(d)){var e=b[d];i f(e.startsWith("$")){e=c[e.substring(1)]}a.logInfo("simpleMsgComposer: Adding new key-vaule to message: "+d+" = "+e);f[d]=e}}return f},passthroughComposer:funct ion(c,b){a.logInfo("datasetComposer: Creating new message");var f={};var e=b.filteredKeys;if(!e){e=[]}for(var d in c){if(e.indexOf(d)>=0){continue}f[d]=c[d]}return f}})(this);this.logInfo("New MsgBusTransport Created")}MsgBusTransport.prototype=ModuleManager.create("transport_template");MsgBusTransport.prototype.const ructor=MsgBusTransport;MsgBusT

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\transport_template.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (1249), with CRLF line terminators
Category:	dropped
Size (bytes):	1461
Entropy (8bit):	5.3380175011956865
Encrypted:	false
SSDEEP:	
MD5:	E26E122B0BACA7D630EF243A99AAC2F7
SHA1:	F93785080E5E672F1AABD2575F83E1A120A5C6F1
SHA-256:	161E501CD97AAFFC1A69CE6DCD1B6D4519F86575745FF215E4C49B8ED2B0654D
SHA-512:	1AB6891B2ED18860B02AE892901AEF93FF19D533E1E654C34E549A76182213C3B8BB6C1B5BA3EA5D8FD6BA90AF1E391DA87853FA5E1342A442F1A3526EA6B52 E
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var transport_template_fileVersion = "1.4.114"; ..function TransportPlugin_Template(){}if(typeof TransportPlugin_Template.prototype. GetName!=="function"){TransportPlugin_Template.prototype={GetName:function(){return this._name},GetVersion:function(){if(transport_template_fileVersion){return transport_template_fileVersion}return"0.0.0"},Initialize:function(b,d,a){try{if(!a||!b||!d){logError("TransportPlugin_Template: Failed to initialize (name). Config: "+a+". Name: "+b+".Dictionary: "+d);return false}this._dictionary=JSON.parse(d);this._config=JSON.parse(a);this._name=b;if(!this._config||!this._name){logError("TransportPlugi n_Template: Failed to initialize (name). Config: "+a+". Name: "+b);return false}return this._setup()}catch(c){logError("TransportPlugin_Template::Initialize Exception caught with message: "+c.message)}},Send:function(a){logError("TransportPlugin_Template::Send: Did not overwrite function. Send will return false");return false},Uninitializ

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\wa_settingsdb.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (814), with CRLF line terminators
Category:	dropped
Size (bytes):	1021
Entropy (8bit):	5.407414719714446
Encrypted:	false
SSDEEP:	
MD5:	17C871882C6C874CA0ED103FF63F3FEE
SHA1:	1F693800FF2C8063EF66F6ADECCCD3C352312649
SHA-256:	F023ED084B8090DEC646B18DE0F7F57D826B5D771459CFA3485B9199AFF88EB5
SHA-512:	255ABF929A8216485243130B08F631BA0D3833AD3933B33849BE75946F8B5C89AAA3E6B7D154D560D6A94F004EF4EE4D1E8ACBEF11F373F1825AB65F1D965741
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var wa_settingsdb_fileVersion = "1.4.114"; ..function CreateWASettingsDBHelper(){var a={getSetting:function(b,c,f){try{logDebug("getting WA setting: "+b);return this._getPlugin().GetSetting(b,c,f)}catch(d){logError("wa_settingsdb:getSetting: "+d.message+"setting("+b+")")}},fetchFromDataDefinition:function(g){try{if(!g){logError("wa_settingsdb:fetchFromDataDefinition Invalid data definition");return null}var b=g.name;var c=g.scope;var f=g["default"];return a.getSetting(b,c,f)}catch(d){logError("wa_settingsdb:fetchFromDataDefinition: "+d.message+"datadefinition("+JSON.stringify(g)+")")}return null},_getPlugin:function(){if(!this._waSettingsDBPlugin){this._waSettingsDBPlugin=getPluginFactory().Create("SettingsDB")}return this._waSettingsDBPlugin},_settingsDBPlugin:null};return a}ModuleManager.registerFactory("wa_settingsdb",CreateWASettingsDBHelper);..//0BCF996CA278776F18D980E1CD65E957514E3AC7C641017A9265F2C11C54BD2992B187E6888F1FCC84B31BBFF02150C555336672D6E3F

C:\ProgramData\McAfee\MSSPlusClientAnalytics\Scripts\wmi.js

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	ASCII text, with very long lines (7401), with CRLF line terminators
Category:	dropped
Size (bytes):	7598
Entropy (8bit):	5.384536988836127
Encrypted:	false
SSDEEP:	
MD5:	574BF04A7290D97FC5C676841AA8580A
SHA1:	0D86A946ED32595A931D14532AA383DA0F99B72D
SHA-256:	A36A85FE02E4DA4C92B5289D03E088900F00A8B61BBFF139DD96253BB22ED99A
SHA-512:	6A6FC615C99EFE69943C5BC749CFB044D5205590894F16C4FF145700F739134B0AC4DD2B284168F04FBAB2CC3470EE48A41DB3DD67A4055F1A48EE0E2E221F3C
Malicious:	false
Reputation:	unknown
Preview:	/*! $FileVersion=1.4.114 */ var wmi_fileVersion = "1.4.114"; ..function CreateWMIManger(){var a={_createAttribute:function(f,c){var g={_data:[],get:function(l,j){try{return l(this._data,j)}catch(k){return null}}};try{f.reset();var d=f.next();while(d){var h=d.get(c);g._data.push(h);d=f.next()}}catch(i){logDebug("failed to populate attribute object")}return g},_getMockIterator:function(){var c={reset:function(){logWarning("mockIterator: Calling reset(). noop")},next:function(){logWarning("mockIterator: Calling next(). Returning `null`");return null}};return c},_unavailableServers:{},resetAvailableServers:function(){this._unavailableServers={}},_getServer:function(g){try{if(this._unavailableServers[g]==true){return null}if(!g){return null}var c=this.getPlugin();if(!c){return null}var f=c.connectServer(g);if(f){return f}}catch(d){logError("_getServer: "+d.message)}this._unavailableServers[g]==true;return null},_queryWMIServer:function(h,d){try{if(!d||!h){return null}var g=this._getServer(h

C:\ProgramData\McAfee\MSSPlusClientAnalytics\dataConfig.cab

Process:	C:\Users\user\Desktop\SecurityScan_Release.exe
File Type:	Microsoft Cabinet archive data, many, 68256 bytes, 44 files, at 0x44 +A "aviary_client.js" +A "common.js", flags 0x4, number 1, extra bytes 20 in head, 17 datablocks, 0x1503 compression
Category:	dropped
Size (bytes):	81360
Entropy (8bit):	7.977829061695821
Encrypted:	false
SSDEEP:	
MD5:	6C9F7102550881FCBB8ACA29B23FAFBD
SHA1:	240DFCC6C4E7E6AC48E27F0E2BF9496A544D03E5
SHA-256:	F3B1783C05D76E950454D9EB26DC8C9092084C77CA0561211BD3CBE43FA6BFB6
SHA-512:	DDCCBA6715A21CA2C0A03A6740FFD953F71447C6F2F1FAFCA9B3CEB2DD124309EC8835807D017CEC6513A986197A5BCEC3A3901A2409C67F471B5AD12CA5902
Malicious:	false
Reputation:	unknown
Preview:	MSCF.....D.....,.....03.....kYE. .aviary_client.js..8.....kYA. .common.js.....?....kYA. .config_manager.js.....C....kYA. .csp_client.js.....Q...kYA. .dataset.js.9)..]n....kY. .datasets_catalog.json.).....kYA. .dataset_da.js..6.....kYA. .data_collector.js..]..I.....kY. .data_items.json.t...\F....kY[. .da_definitions.json..N..K....kYj. .dictionary.json.....kYC. .emitter.js..-..z.....kYA. .engine.js.....kYC. .error_transmitter.js..V..7.....kYx. .events.json.....:....kYA. .event_handler.js.....U....kYB. .hash128.js.....e....kYB. .json2.js.1....t....kYB. .logging.js.:.....kYB. .mappings.js.....kYB. .mcutil.js.....kYl. .observability_datasets.json.....kYB. .observation_analytics.js.P.....kYB. .operations.js.....kYB. .preprocessors.js.Y.....kY.. .profile.json.....`.....kYC. .registry.js.....kYC. .rest_transport.js.u.....kYC. .rules.js.B...g.....kYC. .sha256.js.^.....

C:\Users\user\AppData\Local\Microsoft\TokenBroker\Cache\5a2a7058cf8d1e56c20e6b19a7c48eb2386d141b.tbres	
Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	data
Category:	dropped
Size (bytes):	2278
Entropy (8bit):	3.8535087427459382
Encrypted:	false
SSDEEP:	
MD5:	660266A0A6C793CA580036E2F872A29A
SHA1:	4F6E1EC3431217D1D5F6CA7A3835DACB157BA438
SHA-256:	B95F7C0735B3268A6CA3D8DB0431CDFA093C842C96F5697E34632A175FA1F6CE
SHA-512:	9291AF46C273903D1BE7AC5A93F28626D221D1993F5BDDF3DF9C45FFB81198E11D3528C8ACB0EEEDC2BCAB9D270F5A729D30ADB390A70D1F1FAE9F48F191DB19
Malicious:	false
Reputation:	unknown
Preview:	{.".T.B.D.a.t.a.S.t.o.r.e.O.b.j.e.c.t.".:.{.".H.e.a.d.e.r.".:.{.".O.b.j.e.c.t.T.y.p.e.".:.".T.o.k.e.n.R.e.s.p.o.n.s.e.".,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.a.j.o.r.".:.2.,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.i.n.o.r.".:.1.},.,".O.b.j.e.c.t.D.a.t.a.".:.{.".S.y.s.t.e.m.D.e.f.i.n.e.d.P.r.o.p.e.r.t.i.e.s.".:.{.".R.e.q.u.e.s.t.I.n.d.e.x.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".W.i.p.w.W.M.+.N.H.l.b.C.D.m.s.Z.p.8.S.O.s.j.h.t.F.B.s.=.".},.,".E.x.p.i.r.a.t.i.o.n.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".g.K.y.e.H.x.1.h.2.w.E.=.".},.,".S.t.a.t.u.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".A.A.A.A.A.A.=.=.".},.,".R.e.s.p.o.n.s.e.B.y.t.e.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.t.r.u.e.,.".V.a.l.u.e.".:.".A.Q.A.A.A.N.C.M.n.d.8.B.F.d.E.R.j.H.o.A.w.E./.C.I.+.s.B.A.A.A.A.2.v.e.w.x.4.

C:\Users\user\AppData\Local\Microsoft\TokenBroker\Cache\e8ddd4cbd9c0504aace6ef7a13fa20d04fd52408.tbres	
Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	data
Category:	dropped
Size (bytes):	2684
Entropy (8bit):	3.9010069597209074
Encrypted:	false
SSDEEP:	
MD5:	43A357A9F621EB3277727EBD5243D1BD
SHA1:	E6B25CE325EC42D782A23947ECFC6A3BBBB11790
SHA-256:	FB6F851B38EDBD50D166B12FFBB06FDA876F0D49428D670514E60F10427D2F62
SHA-512:	F618F6C3F0BF274D356688459E0FD9C9030270A3F66C16F6B1D8FE051682C4D1C54AAC5A32B95339643D4848B4F7AF07D4B4C20655F19D80AB4B6331337F888E
Malicious:	false
Reputation:	unknown
Preview:	{.".T.B.D.a.t.a.S.t.o.r.e.O.b.j.e.c.t.".:.{.".H.e.a.d.e.r.".:.{.".O.b.j.e.c.t.T.y.p.e.".:.".T.o.k.e.n.R.e.s.p.o.n.s.e.".,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.a.j.o.r.".:.2.,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.i.n.o.r.".:.1.},.,".O.b.j.e.c.t.D.a.t.a.".:.{.".S.y.s.t.e.m.D.e.f.i.n.e.d.P.r.o.p.e.r.t.i.e.s.".:.{.".R.e.q.u.e.s.t.I.n.d.e.x.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".6.N.3.U.y.9.n.A.U.E.q.s.5.u.9.6.E./.o.g.0.E./.V.J.A.g.=.".},.,".E.x.p.i.r.a.t.i.o.n.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".n.2.r.0.N.u.Z./.3.A.E.=.".},.,".S.t.a.t.u.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".A.A.A.A.A.A.=.=.".},.,".R.e.s.p.o.n.s.e.B.y.t.e.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.t.r.u.e.,.".V.a.l.u.e.".:.".A.Q.A.A.A.N.C.M.n.d.8.B.F.d.E.R.j.H.o.A.w.E./.C.I.+.s.B.A.A.A.A.2.v.e.w.x.4.

C:\Users\user\AppData\Local\Temp\49b434c6-f349-4510-bf13-a106d882086a.tmp	
Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	PNG image data, 62 x 1, 8-bit colormap, non-interlaced
Category:	modified
Size (bytes):	199373
Entropy (8bit):	7.64428818044537
Encrypted:	false
SSDEEP:	
MD5:	06BD1FDF9766D6E08215071B25F882D3
SHA1:	8E744CA886C03A52C90F73A56B602E874FF70524
SHA-256:	76910E5FB1833857C5645DE02624ABDD947D79655C02BF7A1D212929F810C857
SHA-512:	227B37154B18583A4C60331B6BB26B0032FADCAC87504CB039AFFC7F3183CB0E01172233627645715E7D1DB6A71008213EA7431B8296C3F4FFCD1DA376719CCI
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR...>.....3.....pHYs.....MiCCPPhotoshop ICC profile..x.SwX...>..e.VB..I.."#....Y....a...@...V....HU...H...(.gA..Z.U\8....}z.....y.....&..j.9R.<:...OH...H.. ....g.....yx~t.?...o...p..$.....P&W. ..".....R...T.....S.d.....ly\|B".....I>.....(G$.@..`U.R,.....@".....Y.2G.....v.X..@`...B,.. 8..C.... L..0.._p..H.....K.3.....w....!..l.Ba.) .f..".#.H..L.....8?.....f.l....k.o">!.....N...._....p...u.k.[..V.h..]3...Z..z..y8.@...P.<.....%b..0.>.3.o..~..@...z..q.@.....qanv.R....B1n..#.....).4.\,...X..P"M.y.R.D!.....2.....w....O. N....I.~.....X.v.@~.-.....g42y.....@+.....\...L....D..*.A.....a.D@.$.<.B.....A.T.:.....18....\..p..`.....A...a!:..b..".....aH4... ..Q"..r...Bj.]H#.-r.9.\@.... 2....G1.. .Q...u@.....s.t4.]...k....=.....K.ut.}..c..1.f..a\..E`.X.&..c.X5V.5c.X7v....a..$.....^...I...GXLXC.%.#....W...1.'"..O.%z...xb:..XF.&.!.!.%^'._.H$...N.!%.2I.IkH.H-.S.>..i.L&.m.....

C:\Users\user\AppData\Local\Temp\8dc6057b-3f5b-4953-ac94-f9c839cec9a3.tmp	
Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	PNG image data, 590 x 23, 8-bit colormap, non-interlaced
Category:	modified
Size (bytes):	397502
Entropy (8bit):	7.639689704461758
Encrypted:	false
SSDEEP:	
MD5:	82CDA1579396C7448CF844620E95E57D
SHA1:	8C8E257F42ADFC91AEFFCEB6334AA7650F8EAFB6
SHA-256:	9633DDE793C057E00B8D1705B2C79F25F62F20105852C59A2CEA1C82CB6F853F
SHA-512:	2677E746294E57F7C3EC1AFF3D2DB6C1869C7B459007808A87789F912559324378B46C85F392CB698C26110E17F664F50D71FC6A6FA4EDF56896D05ECF8C107E
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR...N.....0.....pHYs.....MiCCPPhotoshop ICC profile..x.SwX...>..e.VB..l.."#....Y....a...@...V....HU...H...(.gA..Z.U\8....}z.....y.....&..j.9R.<:...OH....H.. ....g.....yx~t.?...o...p..$.....P&W. ..."....R...T.....S.d.....ly\|B".....l>.....(G$.@..`U.R,.....@".....Y.2G.....v.X..@`...B,.. 8..C.... L..0.._p..H.....K.3.....w....!..l.Ba.).f.."...#.H..L.....8?.....f.l....k.o">!.....N..._....p...u.k.[..V.h..]3...Z..z..y8.@...P.<.....%b..0.>.3.o..~..@...z..q.@.....qanv.R....B1n..#.....)..4.\,...X..P"M.y.R.D!.....2.....w....O.N....l.~.....X.v.@~.-.....g42y.....@+.....\...L....D..*.A.....a.D@.$.<.B.....A.T.:.....18....\..p..`.....A...a!:..b.."....."aH4... ..Q"..r...Bj.]H#.-r.9.\@.... 2....G1...Q...u@....s.t4.]...k....=.....K.ut.}..c..1.f..a\..E`.X.&..c.X5V.5c.X7v....a..$.....^...I...GXLXC.%.#....W...1.'"..O.%z...xb:..XF.&.!.!.%^'._.H$...N.!%.2I.IkH.H-.S.>..i.L&.m.....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\0bb75071-8faf-4920-ba0f-152ba6c716fe.tmp	
Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	16245
Entropy (8bit):	6.068012164670088
Encrypted:	false
SSDEEP:	
MD5:	4C3DE667DEE72F2EFDBBAC3CAF582CBE
SHA1:	BD9515660B353C68982FF6B066ECD9FF4AC43465
SHA-256:	506DF05C45A9A192A839F3630382274C9B8A7135858973BA79FEA1EE370ECEC8
SHA-512:	9354EC67F36556B42815866DFA083C0AC88F872B62A4C01EA6B1B2B1D7092BA5B5C9A74F3E3B3360EDC2848B4AA6C720F64F701DC07C0C3335F3469357201D6
Malicious:	false
Reputation:	unknown
Preview:	{"domain_actions_config":"H4sIAAAAAAAAAL1dWZPktpH+KxP9ZDtU6GMujfykHY9txVpHyHIoYh2ODhBEkWiCAAdHVbEc/u+bCVb1dE8RqEqOdh806mbzw8VEXshM/PuKb27vha2luF9LHqKT96KVoru3G+mcquXVN/++4sOgleBBWeOvvvnn4YGs7wcLz8erb65+HMKPMVx9dVXbnisDT4wMa612TNj+6j9fUSA+xFpZPyH/9dVVQig59Wx4L5+Cwzjg799ubt/jJP48zeE9TuHwDjYBc/Ew+Ktvbv/z1ZWoe+rsjB4/7Abr5U+ajz9LXo9Px+21Mk1hoo/oX6HHjTLyKTjYyMJmCbLnO/hZMpjFAjSvxOlhbxgi5FK85m+ZCkuQu7UyKoxLO97yIFoYvbAluiw2oRoYgIQ2nG2AqJY2U+koRXQbbMm3fMsEX9JMK3GLbeAvNjhrlo5GOJiTA/oXLTdG6qXtmMBDiyS59PvY7eCklyb4QcfFi7tpdwu3VBt1XNorvM4+RiU6+CjD0kb+pHz7rRm3rXSyzABnWdKBG+Ijlx7hEE4QTzo+AB6fnDLLJBpo7PKv8Ob367/KjUg8mcY6CmCjTJCmtsWFOcUf5vj04cw0e1yZe2WAl8svFn5IC43jfc+dLnGrEyDwAicHCxNdhlrVa5LEtTgt5u2IAK02pd198r5dr5VYgHj55vViEOsF96z3F4ONrN2yeYHGQlo5wvtB8h5moYSz3q4XkgOLF68CtN9bg4RrXXMpaCsrtm158li7QF+b2Xe4pcP9WmmQQPfW3MPK3vutAkF92eZ7P7Xw59TAM/Xo+dJlBvYcfjl+KQYiMwDeq8wvchf+8fPfPPLcZ/KFm8bG4FljbVPigsVWQEqHL2vBay66hdg1F7Kydil8K9Pwl4LVThXUnCL448fFvVayoDCWsdbVqNMUlJkiPsBWAMpciK6VFzCA4g6Ya+AgMj+8/wkfpDfC4Y2ZPYK8UE

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\292fc97d-90fa-4b02-860a-5ae1ae8f7039.tmp	
Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	16335
Entropy (8bit):	6.067483848323677
Encrypted:	false
SSDEEP:	
MD5:	3AD916D115F83128C864534967EEE932
SHA1:	6659D52915818A088745E6BC14819096A89198F5
SHA-256:	A083DAE83FE016BDA85B42E3FCEECC044F05DA7911523818B918847AC8B7F21D
SHA-512:	94E3F20982C5E516352AE8C7FB68251FA3DB5A8B72BA8B05D5AFE2A4F73E40CB9E4732114C8A8DC7063C83D9AE604DC9EBD068F730EF36EAD94CA4BBE8A0C6C6
Malicious:	false
Reputation:	unknown

Preview:	{"domain_actions_config":"H4sIAAAAAAAAAL1dWZPktpH+KxP9ZDtU6GMujfykHY9txVpHyHIoYh2ODhBEkWiCAAdHVbEc/u+bCVb1dE8RqEqOdh806mbzw8VEXshM/PuKb27vha2luF9LHqKT96KVoru3G+mcquXVN/++4sOgleBBWeOvvvnn4YGs7wcLz8erb65+HMKPMVx9dVXbnisDT4wMa612TNj+6j9fUSA+xFpZPyH/9dVVQig59Wx4L5+Cwzjg799ubt/jJP48zeE9TuHwDjYBc/Ew+Ktvbv/z1ZWoe+rsjB4/7Abr5U+ajz9LXo9Px+21Mk1hoo/oX6HHjTLyKTjYyMJmCbLnO/hZMpjFAjSvxOlhbxgi5FK85m+ZCkuQu7UyKoxLO97yIFoYvbAluiw2oRoYgIQ2nG2AqJY2U+koRXQbbMm3fMsEX9JMK3GLbeAvNjhrlo5GOJiTA/oXLTdG6qXtmMBDiyS59PvY7eCklyb4QcfFi7tpdwu3VBt1XNorvM4+RiU6+CjD0kb+pHz7rRm3rXSyzABnWdKBG+Ijlx7hEE4QTzo+AB6fnDLLJBpo7PKv8Ob367/KjUg8mcY6CmCjTJCmtsWFOcUf5vj04cw0e1yZe2WAl8svFn5IC43jfc+dLnGrEyDwAicHCxNdhlrVa5LEtTgt5u2IAK02pd198r5dr5VYgHj55vViEOsF96z3F4ONrN2yeYHGQlo5wvtB8h5moYSz3q4XkgOLF68CtN9bg4RrXXMpaCsrtm158li7QF+b2Xe4pcP9WmmQQPfW3MPK3vutAkF92eZ7P7Xw59TAM/Xo+dJlBvYcfjI+KQYiMwDeq8wvchf+8fPfPPLcZ/KFm8bG4FljbVPigsVWQEqHL2vBay66hdg1F7Kydil8K9Pwl4LVThXUnCL448fFvVayoDCWsdbVqNMUlJkiPsBWAMpciK6VFzCA4g6Ya+AgMj+8/wkfpDfC4Y2ZPYK8UE

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\319b4a06-297c-4545-bce3-3f1f7cb93364.tmp

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	JSON data
Category:	modified
Size (bytes):	17648
Entropy (8bit):	6.060281485412487
Encrypted:	false
SSDEEP:	
MD5:	E73DF99B52437832F67BD61654DCC680
SHA1:	4AF333CD516BB94960D90002B9FA5A2F1920AE86
SHA-256:	A5FC0F9C86994668E779C5175A501C4E46D375F465B0E763A62680ACB50473C3
SHA-512:	60F6BBF4AC59C320EFAF2BD3CD3A35EA08F8ADC608D8E38895D70BA67660AF33DD4B486C3F45DB290B61B29AC35CEDB6FBDAFC090BAD6F26FF8E889426D4 47F
Malicious:	false
Reputation:	unknown
Preview:	{"desktop_session_duration_tracker":{"last_session_end_timestamp":"1736262015"},"domain_actions_config":"H4sIAAAAAAAAAL1dWZPktpH+KxP9ZDtU6GM ujfykHY9txVpHyHIoYh2ODhBEkWiCAAdHVbEc/u+bCVb1dE8RqEqOdh806mbzw8VEXshM/PuKb27vha2luF9LHqKT96KVoru3G+mcquXVN/++4sOgleBBWeO vvvnn4YGs7wcLz8erb65+HMKPMVx9dVXbnisDT4wMa612TNj+6j9fUSA+xFpZPyH/9dVVQig59Wx4L5+Cwzjg799ubt/jJP48zeE9TuHwDjYBc/Ew+Ktvbv/z1ZWoe+rsj B4/7Abr5U+ajz9LXo9Px+21Mk1hoo/oX6HHjTLyKTjYyMJmCbLnO/hZMpjFAjSvxOlhbxgi5FK85m+ZCkuQu7UyKoxLO97yIFoYvbAluiw2oRoYgIQ2nG2AqJY2U+koRXQ bbMm3fMsEX9JMK3GLbeAvNjhrlo5GOJiTA/oXLTdG6qXtmMBDiyS59PvY7eCklyb4QcfFi7tpdwu3VBt1XNorvM4+RiU6+CjD0kb+pHz7rRm3rXSyzABnWdKBG+Ijlx7hE E4QTzo+AB6fnDLLJBpo7PKv8Ob367/KjUg8mcY6CmCjTJCmtsWFOcUf5vj04cw0e1yZe2WAl8svFn5IC43jfc+dLnGrEyDwAicHCxNdhlrVa5LEtTgt5u2IAK02pd198r5 dr5VYgHj55vViEOsF96z3F4ONrN2yeYHGQlo5wvtB8h5moYSz3q4XkgOLF68CtN9bg4RrXXMpaCsrtm158li7QF+b2Xe4pcP9WmmQQPfW3MPK3vutAkF92eZ 7P7Xw59TAM/Xo+dJlBvYcfjI+KQYiMwDeq8wvchf+8fPfPPLcZ/KFm8bG4FljbVPigsVWQEqHL2vBay66hdg1F7Kydil8K9Pwl4L

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\37d1dd6a-bd8e-499e-b432-b4f1ec581747.tmp

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	17662
Entropy (8bit):	6.059972893977599
Encrypted:	false
SSDEEP:	
MD5:	27D6D98BB866F08F5D3CD052ED292752
SHA1:	18B6C5C03A6CEF2A988326690FE27B9E48D7A56D
SHA-256:	72AADDFE3D20954F43154641CF1BD858FAD64796B073B31B3BB3EFCD5EBAE254
SHA-512:	3B57558E30276C81645FB0BFCFA241E21C2F0F943C0DB27ABE4ED8A2C01BF9BAD805DF9620D491ABC72CCA85D7263206151CC10222923B3C0EF930B4051403 3
Malicious:	false
Reputation:	unknown
Preview:	{"desktop_session_duration_tracker":{"last_session_end_timestamp":"1736262041"},"domain_actions_config":"H4sIAAAAAAAAAL1dWZPktpH+KxP9ZDtU6GM ujfykHY9txVpHyHIoYh2ODhBEkWiCAAdHVbEc/u+bCVb1dE8RqEqOdh806mbzw8VEXshM/PuKb27vha2luF9LHqKT96KVoru3G+mcquXVN/++4sOgleBBWeO vvvnn4YGs7wcLz8erb65+HMKPMVx9dVXbnisDT4wMa612TNj+6j9fUSA+xFpZPyH/9dVVQig59Wx4L5+Cwzjg799ubt/jJP48zeE9TuHwDjYBc/Ew+Ktvbv/z1ZWoe+rsj B4/7Abr5U+ajz9LXo9Px+21Mk1hoo/oX6HHjTLyKTjYyMJmCbLnO/hZMpjFAjSvxOlhbxgi5FK85m+ZCkuQu7UyKoxLO97yIFoYvbAluiw2oRoYgIQ2nG2AqJY2U+koRXQ bbMm3fMsEX9JMK3GLbeAvNjhrlo5GOJiTA/oXLTdG6qXtmMBDiyS59PvY7eCklyb4QcfFi7tpdwu3VBt1XNorvM4+RiU6+CjD0kb+pHz7rRm3rXSyzABnWdKBG+Ijlx7hE E4QTzo+AB6fnDLLJBpo7PKv8Ob367/KjUg8mcY6CmCjTJCmtsWFOcUf5vj04cw0e1yZe2WAl8svFn5IC43jfc+dLnGrEyDwAicHCxNdhlrVa5LEtTgt5u2IAK02pd198r5 dr5VYgHj55vViEOsF96z3F4ONrN2yeYHGQlo5wvtB8h5moYSz3q4XkgOLF68CtN9bg4RrXXMpaCsrtm158li7QF+b2Xe4pcP9WmmQQPfW3MPK3vutAkF92eZ 7P7Xw59TAM/Xo+dJlBvYcfjI+KQYiMwDeq8wvchf+8fPfPPLcZ/KFm8bG4FljbVPigsVWQEqHL2vBay66hdg1F7Kydil8K9Pwl4L

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\43e42eab-b009-423a-9b13-3b1bee00c322.tmp

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	16245
Entropy (8bit):	6.068008163090177
Encrypted:	false
SSDEEP:	
MD5:	265B83B0ABDFB5792AB432512DF27B6D

SHA1:	D4201B7949A7A65397A8A0C78482A77481C59DA0
SHA-256:	3A7A256684896305772599229154AB2990742C5C7A70F610F0B17D6B5897F05F
SHA-512:	D7E202437F11518D980E245EE231F6E8526D7930113AB1148324247C8FBF626F1BC77A9CB005649ABD8E98992CC6732DEB63FC0C84390F0477DF5AA9421BD2C(
Malicious:	false
Reputation:	unknown
Preview:	{"domain_actions_config":"H4sIAAAAAAAAAL1dWZPktpH+KxP9ZDtU6GMujfykHY9txVpHyHIoYh2ODhBEkWiCAAdHVbEc/u+bCVb1dE8RqEqOdh806mbzw8VEXshM /PuKb27vha2luF9LHqKT96KVoru3G+mcquXVN/++4sOgleBBWeOvvvnn4YGs7wcLz8erb65+HMKPMVx9dVXbnisDT4wMa612TNj+6j9fUSA+xFpZPyH/9dVVQig59Wx4L5 +Cwzjg799ubt/jJP48zeE9TuHwDjYBc/Ew+Ktvbv/z1ZWoe+rsjB4/7Abr5U+ajz9LXo9Px+21Mk1hoo/oX6HHjTLyKTjYyMJmCbLnO/hZMpjFAjSvxOlhbxgi5FK85m+Z CkuQu7UyKoxLO97yIFoYvbAluiw2oRoYgIQ2nG2AqJY2U+koRXQbbMm3fMsEX9JMK3GLbeAvNjhrlo5GOJiTA/oXLTdG6qXtmMBDiyS59PvY7eCklyb4QcfFi7tpdwu3VB t1XNorvM4+RiU6+CjD0kb+pHz7rRm3rXSyzABnWdKBG+Ijlx7hEE4QTzo+AB6fnDLLJBpo7PKv8Ob367/KjUg8mcY6CmCjTJCmtsWFOcUf5vj04cw0e1yZe2WAl8svFn5I C43jfc+dLnGrEyDwAicHCxNdhlrVa5LEtTgt5u2lAK02pd198r5dr5VYgHj55vViEOsF96z3F4ONrN2yeYHGQlo5wvtB8h5moYSz3q4XkgOLF68CtN9bg4RrXXMpaCsrtm 158li7QF+b2Xe4pcP9WmmQQPfW3MPK3vutAkF92eZ7P7Xw59TAM/Xo+dJlBvYcfjl+KQYiMwDeq8wvchf+8fPfPPLcZ/KFm8bG4FljbVPigsVWQEqHL2vBay66hdg1F7Ky dil8K9Pwl4LVThXUnCL448fFvVayoDCWsdbVqNMUlJkiPsBWAMpciK6VFzCA4g6Ya+AgMj+8/wkfpDfC4Y2ZPYK8UE

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\817a63fe-de7c-46d2-8d0d-0cdb4d179274.tmp

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	2899
Entropy (8bit):	5.297467803596752
Encrypted:	false
SSDEEP:	
MD5:	F09904CD88C8A4CBBBA6DE5330A5F932
SHA1:	A81170A2692D9A0760DC9420D775B633A0860F69
SHA-256:	DB867C93884D453F93AEABC9951860E72483E026E061FFA7993191556CE49BE2
SHA-512:	2D460858F5705B2EDD32D81B66DDBAB9FE2F8B7901B22D62256566DA7117B8B659688C210A0CF431D2406031BE0248013FA370C01127999E7AC0C175CB8391CA
Malicious:	false
Reputation:	unknown
Preview:	{"dual_engine":{"ie_to_edge":{"redirection_mode":0}},"edge":{"tab_stabs":{"closed_without_unfreeze_never_unfrozen":0,"closed_without_unfreeze_previously_unfroze n":0,"discard_without_unfreeze_never_unfrozen":0,"discard_without_unfreeze_previously_unfrozen":0},"tab_stats":{"frozen_daily":0,"unfrozen_daily":0}},"fre":{"oe m_bookmarks_set":true},"hardware_acceleration_mode_previous":true,"legacy":{"profile":{"name":{"migrated":true}}},"os_crypt":{"audit_enabled":true,"encrypted_ke y":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAADa97DHgF1bTLB8B82Kj8teEAAAAB4AAABNAGkAYwByAG8AcwBvAGYAdAAgAEUAZABnAGUAAAAQZgAA AAEAACAAAAAlrx1Cjya7uJDm1MwCHVdt/NvSdippGJsSw9f21MAgIQAAAAAOgAAAAIAACAAAAAT/eDRHZsAx4uG4YeQ8G1SbqKPgSaFYIAJ65+yDjZfZzAA AAAUfKEvsQ2T0STJlHVA/9JbtE280SyoQpiydlkC2kJWGmmWEljP35x5N7kfI6z59kFAAAAAiktMt75lJcYYWoPlPhhbaJnvvQfuyDUrKC7Y++AxHgKr8bnoXfSBWZKk7N 5/l7FduXlABYM361cxKsoYrwB6lA=="},"policy":{"last_statistics_update":"13380735557999359"},"profile":{"info_cache":{"Default":{"avatar_icon":"chrome://t

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Crashpad\settings.dat

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	data
Category:	dropped
Size (bytes):	280
Entropy (8bit):	1.860216996293906
Encrypted:	false
SSDEEP:	
MD5:	926AA92609B680B6F48A96E5820706D6
SHA1:	511789EEC893A679500B26982E941E127F0F5F86
SHA-256:	0999D9428A134693585389B899C76E5831ED4599CDB0CA8115D5FDE2F22D1FB2
SHA-512:	F7F01F5E7E600CD569A7CC9170941EF5D6E62CDE24A3B0E97068F8BC7AC900FBB645730A84F47874FEF0FC7EF5A359CA33DA0AD0AC923BF5E78D73585AD594 7D
Malicious:	false
Reputation:	unknown
Preview:	sdPC.....sC..3.F..o.x.....{F3017226-FE2A-4295-8BDF-00C3A9A7E4C.}C:.....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Crashpad\throttle_store.dat

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	20
Entropy (8bit):	3.6219280948873624
Encrypted:	false
SSDEEP:	
MD5:	9E4E94633B73F4A7680240A0FFD6CD2C

SHA1:	E68E02453CE22736169A56FDB59043D33668368F
SHA-256:	41C91A9C93D76295746A149DCE7EBB3B9EE2CB551D84365FFF108E59A61CC304
SHA-512:	193011A756B2368956C71A9A3AE8BC9537D99F52218F124B2E64545EEB5227861D372639052B74D0DD956CB33CA72A9107E069F1EF332B9645044849D14AF337
Malicious:	false
Reputation:	unknown
Preview:	level=none expiry=0.

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\6701d20b-4faa-4a46-b021-cb5373b4327c.tmp

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	6780
Entropy (8bit):	5.579621677752821
Encrypted:	false
SSDEEP:	
MD5:	C6B5583BAB121EB07E2712B582741EB9
SHA1:	7661020BB15CD19F33AD772B1473DA7EE1D4E972
SHA-256:	078574FB4E90062C6EDE4970549C6CD1874547723D2FE9276360877AA88BF71A
SHA-512:	320A09647492F330C4285B8C1EA23A2B93AF462D5A9700A8D03FD780D13DF7591ABB18E73D890371FF2FCF4347B30FE32F665A47EB3032FFA0080E4AF0A255C6
Malicious:	false
Reputation:	unknown
Preview:	{"extensions":{"settings":{"dgiklkfkllikcanfonkcabmbdfmgleag":{"active_permissions":{"api":[],"explicit_host":[],"manifest_permissions":[],"scriptable_host":[]},"commands":{},"content_settings":[],"creation_flags":1,"events":[],"first_install_time":"13380735558068925","from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"last_update_time":"13380735558068925","location":5,"manifest":{"content_capabilities":{"include_globs":["https://*excel.officeapps.live.com/*","https://*onenote.officeapps.live.com/*","https://*powerpoint.officeapps.live.com/*","https://*word-edit.officeapps.live.com/*","https://*excel.officeapps.live.com.mcas.ms/*","https://*onenote.officeapps.live.com.mcas.ms/*","https://*word-edit.officeapps.live.com.mcas.ms/*","https://*excel.partner.officewebapps.cn/*","https://*onenote.partner.officewebapps.cn/*","https://*powerpoint.partner.officewebapps.cn/*","https://*word-edit.partner.officewebapps.cn/*","https://*excel.gov.online.office365.us/*",""

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\84eed6ac-c24a-45d5-97d6-cd3f93b14496.tmp

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	6261
Entropy (8bit):	4.796163590898133
Encrypted:	false
SSDEEP:	
MD5:	6AABE3FAD205437FE406DBC67538C559
SHA1:	C6B5CC414C838DFA2FEED191CF27CA1749CB9BBE
SHA-256:	2A3229402EF711B32F9E3725088338D5FA8F7D476F80449E500286704F450C1C
SHA-512:	1ABCB20B0A3275FB292E5CD5F7C042B23CE1D94C734006EE564B22C635A51BE937C3ADAD6EACD31E5FF8514BF7AF9DAEE1EF97E5FFC0BD0C56E782824A6D20EB
Malicious:	false
Reputation:	unknown
Preview:	{"aadc_info":{"age_group":0},"account_tracker_service_last_update":"13380735558655869","alternate_error_pages":{"backup":true,"enabled":false},"autocomplete":{"retention_policy_last_version":117},"autofill":{"autostuff_enabled":false,"credit_card_enabled":false,"custom_data_enabled":false,"custom_data_fill_enabled":false,"custom_data_identify_info_from_form_enabled":false,"custom_data_save_enabled":false,"profile_enabled":false},"browser":{"available_dark_theme_options":"All","has_seen_welcome_page":false},"browser_content_container_height":450,"browser_content_container_width":550,"browser_content_container_x":0,"browser_content_container_y":0,"countryid_at_install":17224,"credentials_enable_service":false,"dips_timer_last_update":"13380735558583517","domain_diversity":{"last_reporting_timestamp":"13380735558654978"},"dual_engine":{"consumer_mode":{"ie_user":false},"consumer_site_list_with_ie_entries":false,"consumer_sitelist_location":"","consumer_sitelist_version":"","external_consu

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\9e2579e3-3b1a-498f-9923-ae1b6b7e77d9.tmp

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	5791
Entropy (8bit):	4.771637178880713
Encrypted:	false
SSDEEP:	
MD5:	B09FE06EAA190E695AFE7E67D4D66170
SHA1:	BCD13B9014F7D7D511C81EEB5D47AC3C2DA5DBFF
SHA-256:	E975CCDC7366B6F93C2069B22936C1DD1CDCEE278E5280348DF55060E3CD437A

SHA-512:	5CD07EA1FF091AABBAD65923A82410A3261070CA352C4F5D46894DC38E161A64DE66C6A12F7B46C9D02B290AB649B8E78D611B16158D2D1EC21842B7827DAE3
Malicious:	false
Reputation:	unknown
Preview:	{"aadc_info":{"age_group":0},"account_tracker_service_last_update":"13380735558655869","alternate_error_pages":{"backup":true,"enabled":false},"autocomplete":{"retention_policy_last_version":117},"autofill":{"autostuff_enabled":false,"credit_card_enabled":false,"custom_data_enabled":false,"custom_data_fill_enabled":false,"custom_data_identify_info_from_form_enabled":false,"custom_data_save_enabled":false,"profile_enabled":false},"browser":{"available_dark_theme_options":"All","has_seen_welcome_page":false},"browser_content_container_height":450,"browser_content_container_width":550,"browser_content_container_x":0,"browser_content_container_y":0,"countryid_at_install":17224,"credentials_enable_service":false,"dips_timer_last_update":"13380735558583517","domain_diversity":{"last_reporting_timestamp":"13380735558654978"},"dual_engine":{"consumer_mode":{"ie_user":false},"consumer_site_list_with_ie_entries":false,"consumer_sitelist_location":"","consumer_sitelist_version":"","external_consu

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\AssistanceHome\AssistanceHomeSQLite

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 3, cookie 0x1, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	0.3202460253800455
Encrypted:	false
SSDEEP:	
MD5:	40B18EC43DB334E7B3F6295C7626F28D
SHA1:	0E46584B0E0A9703C6B2EC1D246F41E63AF2296F
SHA-256:	85E961767239E90A361FB6AA0A3FD9DAA57CAAF9E30599BB70124F1954B751C8
SHA-512:	8BDACDC4A9559E4273AD01407D5D411035EECD927385A51172F401558444AD29B5AD2DC5562D1101244665EBE86BBDDE072E75ECA050B051482005EB6A52CDD
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Cache\Cache_Data\data_1

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	data
Category:	modified
Size (bytes):	270336
Entropy (8bit):	0.0018164538716206493
Encrypted:	false
SSDEEP:	
MD5:	8EBEE7ED2A2E29A48CE61157B42D6427
SHA1:	9BC0E17A8FE922A145C2A9B8F3F0EF707E4A4008
SHA-256:	AE5346C9BFD9FE450194DE2332C3F6FA180F2FA6D2D831CFA3AE087566CF2530
SHA-512:	1601C2F002A5D7E201F76BDA6D8240C7850D1F8B06B7D89A309B23BFEB0122A036D863D7E802D2AF6BC072ECEC9D9A5C97292CA985511C07239E3E1E442238F
Malicious:	false
Reputation:	unknown
Preview:	....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Cache\Cache_Data\index

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	FoxPro FPT, blocks size 768, next free block index 3284796353, field type 0
Category:	dropped
Size (bytes):	524656
Entropy (8bit):	5.027445846313988E-4
Encrypted:	false
SSDEEP:	
MD5:	B0C6943BA45922DDFDEA9CCBA1CB8CF5
SHA1:	133686215A7B0D556A7C793FBAF71482662C6B3E
SHA-256:	F5941D49CE9CEBEFDE0BCBE2142B2820B525E5ECA954CDED3DF1D8698F563E96

SHA-512:	4886A86937D1338826CE1E86D8EA4206E1918425AC2709B656E81E3C5D4F659EDEA9F46ED236697E13F71E41883B7F28D1E1FCA9A68EFE26CCE4BF9792A1E2D1
Malicious:	false
Reputation:	unknown
Preview:	.....F../.....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Code Cache\js\index

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	2.1431558784658327
Encrypted:	false
SSDEEP:	
MD5:	54CB446F628B2EA4A5BCE5769910512E
SHA1:	C27CA848427FE87F5CF4D0E0E3CD57151B0D820D
SHA-256:	FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D
SHA-512:	8F6ED2E91AED9BD415789B1DBE591E7EAB29F3F1B48FDFA5E864D7BF4AE554ACC5D82B4097A770DABC228523253623E4296C5023CF48252E1B94382C43123CB0
Malicious:	false
Reputation:	unknown
Preview:	0\r..m.....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Code Cache\js\index-dir\temp-index

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	data
Category:	dropped
Size (bytes):	48
Entropy (8bit):	2.9972243200613975
Encrypted:	false
SSDEEP:	
MD5:	3F3260EFAA9BE5463AF07D865B3E5278
SHA1:	299C254BE1AC0B1A6FB6F9C2C8AAF0A77679786F
SHA-256:	EB49B5D20DB377DE633665052E9763AB65E45AD4DEB7C99580CDACE964C0BFEB
SHA-512:	B92FFCBB9BA90F64BDA7E0EF15DEB0C82FF3606DDD22ED32C78F4B93D44333626A0627E9D7680B5E1A0063571B0FD716BB045F9841480ADB1F72B5F6DD13B7B7
Malicious:	false
Reputation:	unknown
Preview:	(....g%oy retne.....E../.

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Code Cache\js\index-dir\the-real-index (copy)

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	
MD5:	3F3260EFAA9BE5463AF07D865B3E5278
SHA1:	299C254BE1AC0B1A6FB6F9C2C8AAF0A77679786F
SHA-256:	EB49B5D20DB377DE633665052E9763AB65E45AD4DEB7C99580CDACE964C0BFEB
SHA-512:	B92FFCBB9BA90F64BDA7E0EF15DEB0C82FF3606DDD22ED32C78F4B93D44333626A0627E9D7680B5E1A0063571B0FD716BB045F9841480ADB1F72B5F6DD13B7B7
Malicious:	false
Reputation:	unknown
Preview:	(....g%oy retne.....E../.

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Code Cache\wasm\index-dir\temp-index	
Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	data
Category:	dropped
Size (bytes):	48
Entropy (8bit):	2.9138909867280645
Encrypted:	false
SSDEEP:	
MD5:	031496C8B861DC917385C8273FDC986D
SHA1:	80C9E1E141DB486BEB24E7615982285C84CAFAEE
SHA-256:	F3F25604E8DEE779EDFDF92AC9CB924ACD9F7ACEAAF653788B949FB02DED4BFE
SHA-512:	7DCC2AF5CA6F3CB185552B246A11DCC1214F7D38487C1E1F389F82584DAD2BA63AF157237E5BD7EF6DC40BC9AEEF244BE6BA82CE260BE8D9DFE625E62122E 24F
Malicious:	false
Reputation:	unknown
Preview:	(...E...oy retne.....E../.

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Code Cache\wasm\index-dir\the-real-index (copy)	
Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	
MD5:	031496C8B861DC917385C8273FDC986D
SHA1:	80C9E1E141DB486BEB24E7615982285C84CAFAEE
SHA-256:	F3F25604E8DEE779EDFDF92AC9CB924ACD9F7ACEAAF653788B949FB02DED4BFE
SHA-512:	7DCC2AF5CA6F3CB185552B246A11DCC1214F7D38487C1E1F389F82584DAD2BA63AF157237E5BD7EF6DC40BC9AEEF244BE6BA82CE260BE8D9DFE625E62122E 24F
Malicious:	false
Reputation:	unknown
Preview:	(...E...oy retne.....E../.

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\DIPS	
Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 7, cookie 0x3, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.43508159006069336
Encrypted:	false
SSDEEP:	
MD5:	F5237AED0F897E7619A94843845A3EC3
SHA1:	A0C752C9C28A753CFB051AACE2ADA78A6D1288C3
SHA-256:	D4463972AD7B1582F05C8E17074CE863D45CA625C2C672DB0D37F3AF4C7ACE42
SHA-512:	D3C9718794E455D415D8EDF23B576E0A70356B8D71B8DD374D25B8065FEF608E114E13395B4B54462739882A141F4DBE00E3A370D6E4160504428A849CC893A3
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....j.....g.....8...n..... ....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\DawnCache\data_1	
Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0018164538716206493

Encrypted:	false
SSDEEP:	
MD5:	819514E4097DFBE58AFAD47F437BB136
SHA1:	F5F579817F9EF7633CD603346970E28DB2884BC1
SHA-256:	E8FEBD142BB807AD78FC77071036ACEF177F5C4BFE1F70D6CFB4AE1B19685ABC
SHA-512:	6A5AAC0D6E2B3FBA5643C1AFD844C6C1CBA07F4BABCDA36EA13D3A668F37A21F0A05891D7CCFBCC2DAB16F686AC50364286722A913662A4220CFBD7F4BB3 1A3
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\DawnCache\data_3

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.012340643231932763
Encrypted:	false
SSDEEP:	
MD5:	41876349CB12D6DB992F1309F22DF3F0
SHA1:	5CF26B3420FC0302CD0A71E8D029739B8765BE27
SHA-256:	E09F42C398D688DCE168570291F1F92D079987DEDA3099A34ADB9E8C0522B30C
SHA-512:	E9A4FC1F7CB6AE2901F8E02354A92C4AAA7A53C640DCF692DB42A27A5ACC2A3BFB25A0DE0EB08AB53983132016E7D43132EA4292E439BB636AAFD53FB6EF9 07E
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\DawnCache\index

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	FoxPro FPT, blocks size 768, next free block index 3284796353, field type 0
Category:	dropped
Size (bytes):	262512
Entropy (8bit):	9.553120663130604E-4
Encrypted:	false
SSDEEP:	
MD5:	F3C5F2D5195A9DB68018B1B4A4E129A0
SHA1:	64DAEBB55403625F31E8BF53D143C48F2233F164
SHA-256:	6B2F9CADE2781AA5F99C27CE0D3305528A5BE810588FA9495C686511DCEEF509
SHA-512:	A6987FC3070465B74FAE4216C6A0A9CCD8DADF543635B8DF8B7FEC9B7637452994CC7F819D1CB3657D02E93C5134147705A291698E6B3F99C3AE80722E98297
Malicious:	false
Reputation:	unknown
Preview:	.....G..E../.....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\EdgeEDrop\EdgeEDropSQLite.db

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 14, database pages 8, cookie 0xe, schema 4, UTF-8, version-valid-for 14
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.494709561094235
Encrypted:	false
SSDEEP:	
MD5:	CF7760533536E2AF66EA68BC3561B74D

SHA1:	E991DE2EA8F42AE7E0A96A3B3B8AF87A689C8CCD
SHA-256:	E1F183FAE5652BA52F5363A7E28BF62B53E7781314C9AB76B5708AF9918BE066
SHA-512:	38B15FE7503F6DFF9D39BC74AA0150A7FF038029F973BE9A37456CDE6807BCBDEAB06E624331C8DFDABE95A5973B0EE26A391DB2587E614A37ADD500464701 2
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....j...i.....t...c..... ....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Extension Rules\000003.log

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	
MD5:	51A2CBB807F5085530DEC18E45CB8569
SHA1:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985DI
Malicious:	false
Reputation:	unknown
Preview:	.f.5.....f.5.....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Extension Rules\LOG

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	279
Entropy (8bit):	5.284793778232598
Encrypted:	false
SSDEEP:	
MD5:	BB3215F5FA2A093DAF2390CF6B72F953
SHA1:	4303E8EA28B3781F5A3AF1193E98C750B1D9FE29
SHA-256:	40B469916C2566DB3B72E313D83EF46991ECA4B259F9091EBDD79F6D82039750
SHA-512:	6A5D7F60289369D32AFA8BF870E3EAE5EA7EC07BCBD73EE9791FF4D9D97149B0CE783C6B1A77C18947C29C1A2A70522802E0C57F8C808A27076D5CA2EAD354 6F
Malicious:	false
Reputation:	unknown
Preview:	2025/01/07-09:59:18.069 1810 Creating DB C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Extension Rules since it was missing..2025/01/07-09:59:18.159 1810 Reusing MANIFEST C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Extension Rules/MANIFEST-000001.

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Extension Scripts\LOG

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	283
Entropy (8bit):	5.299068820374491
Encrypted:	false
SSDEEP:	
MD5:	292E354FFCE945FC4E19C1AEAABCFB14
SHA1:	F5A4D494EDEC8BBEC4359D693C667F7EB6B78B8A
SHA-256:	C570344C3AC40D2AB676A491939FA37EE42FD26F9112DAA8A15D1DCE310E2985
SHA-512:	1117C60115DB0D9A30CA9FF547F52E3E9BFD9DF3F5686479A60A671618B6CD7F2A183A613639F7C1AB590B29D5753B00493FE27FF07B405F953A8121B34E415C
Malicious:	false
Reputation:	unknown
Preview:	2025/01/07-09:59:18.313 1810 Creating DB C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Extension Scripts since it was missing..2025/01/07-09:59:18.431 1810 Reusing MANIFEST C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Extension Scripts/MANIFEST-000001.

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Extension State\000003.log	
Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	
MD5:	891A884B9FA2BFF4519F5F56D2A25D62
SHA1:	B54A3C12EE78510CB269FB1D863047DD8F571DEA
SHA-256:	E2610960C3757D1757F206C7B84378EFA22D86DCF161A98096A5F0E56E1A367E
SHA-512:	CD50C3EE4DFB9C4EC051B20DD1E148A5015457EE0C1A29FFF482E62291B32097B07A069DB62951B32F209FD118FD77A46B8E8CC92DA3EAAE6110735D126A90EE
Malicious:	false
Reputation:	unknown
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Extension State\LOG	
Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	277
Entropy (8bit):	5.307942835397087
Encrypted:	false
SSDEEP:	
MD5:	F65920FE565029B5AD968D8B6D7E5310
SHA1:	8CF0EA43D75C27E0EC754811B5D190C88367ED9F
SHA-256:	C717A5CD996A1E4D529676E9675F90E969D404C2856363BEFC25B918C0AB77FC
SHA-512:	95115BBFA757A0B44585A3DB5088ECDDE77D5C456CFC8EEB41044A971D973A1FB946AE1BDEBA7F68A12DC2598F23878211E025648B9D24DAE7ED2372E8874412
Malicious:	false
Reputation:	unknown
Preview:	2025/01/07-09:59:18.734 738 Creating DB C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Extension State since it was missing..2025/01/07-09:59:18.779 738 Reusing MANIFEST C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Extension State/MANIFEST-000001.

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\ExtensionActivityComp	
Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 1, cookie 0x1, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.3169096321222068
Encrypted:	false
SSDEEP:	
MD5:	2554AD7847B0D04963FDAE908DB81074
SHA1:	F84ABD8D05D7B0DFB693485614ECF5204989B74A
SHA-256:	F6EF01E679B9096A7D8A0BD8151422543B51E65142119A9F3271F25F966E6C42
SHA-512:	13009172518387D77A67BBF86719527077BE9534D90CB06E7F34E1CCE7C40B49A185D892EE859A8BAFB69D5EBB6D667831A0FAFBA28AC1F44570C8B68F8C90A4
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\ExtensionActivityEdge	
Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 2, database pages 8, cookie 0x8, schema 4, UTF-8, version-valid-for 2
Category:	dropped

Size (bytes):	32768
Entropy (8bit):	0.40981274649195937
Encrypted:	false
SSDEEP:	
MD5:	1A7F642FD4F71A656BE75B26B2D9ED79
SHA1:	51BBF587FB0CCC2D726DDB95C96757CC2854CFAD
SHA-256:	B96B6DDC10C29496069E16089DB0AB6911D7C13B82791868D583897C6D317977
SHA-512:	FD14EADCF5F7AB271BE6D8EF682977D1A0B5199A142E4AB353614F2F96AE9B49A6F35A19CC237489F297141994A4A16B580F88FAC44486FCB22C05B2F1C3F7D1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....j.....M.....8...b.....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Favicons

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 10, cookie 0x8, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6975083372685086
Encrypted:	false
SSDEEP:	
MD5:	F5BBD8449A9C3AB28AC2DE45E9059B01
SHA1:	C569D730853C33234AF2402E69C19E0C057EC165
SHA-256:	825FF36C4431084C76F3D22CE0C75FA321EA680D1F8548706B43E60FCF5B566E
SHA-512:	96ACDED5A51236630A64FAE91B8FA9FAB43E22E0C1BCB80C2DD8D4829E03FBFA75AA6438053599A42EC4BBCF805BF0B1E6DFF9069B2BA182AD0BB30F2542FD3F
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....j.....g....._.c...~.2.....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\GPUCache\data_1

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0018164538716206493
Encrypted:	false
SSDEEP:	
MD5:	1D3A84E1FFC5EF1F0C159392157CDAA9
SHA1:	77602A19A3C5D63D22767DC4A2B0F8F66F3375E7
SHA-256:	F3EB5121AAC02A6EE6FA5D104329590C89BF7A11165ECE7C3645E0B78498C273
SHA-512:	B4B1DF37951D4BD0B92480E4632B53D467ECEA359479A8BFA1FA6BA215FDA0C169475231BDFD03091058A52F7EB19397445707DC34FAA3F89C16E44D3D8703D5
Malicious:	false
Reputation:	unknown
Preview:	

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\GPUCache\index

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	FoxPro FPT, blocks size 768, next free block index 3284796353, field type 0
Category:	dropped
Size (bytes):	262512
Entropy (8bit):	9.553120663130604E-4

Encrypted:	false
SSDEEP:	
MD5:	66944F55E3C0B0012D96BFAFC2A30822
SHA1:	2360C2E10E64AFDD4E21658919F92C8B54B36856
SHA-256:	CAE34EE8142389E3E79F474B7B6FB5601232E7C2885BD1355A9170FB0BC07688
SHA-512:	8C1258AF37C26FA5F4AA7E19BB2115B172D944E1C3C6184DC1802F681741D9F66D430F3DFC3BFE14F21EB330CC8E5E5686C600665E7575D1123EAD6132E45A3
Malicious:	false
Reputation:	unknown
Preview:	.....H..E../..... ....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\History

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 2, database pages 38, cookie 0x1f, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	155648
Entropy (8bit):	0.6821070839392155
Encrypted:	false
SSDEEP:	
MD5:	65DD8E92472964BEF07CDA83E0A90EB7
SHA1:	502A678CFA13621C87020F92C55C54CE44481EDE
SHA-256:	3C0333E9DA578D0C9D094B2633A21DB1102DBEF9045982EBA2B04D542CD8BB25
SHA-512:	E2322FEB628B803934BE49E2C8A0CA277BC78C7FE394F63CCD12F7C21397763ACAF05C32DB7C55006A683EB39333205D6DDE08BEBD8FE097337D842F177EB90
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....&.....j..... ....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Local Storage\leveldb\LOG

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	ASCII text
Category:	modified
Size (bytes):	291
Entropy (8bit):	5.316589927548284
Encrypted:	false
SSDEEP:	
MD5:	61A1FEBC7A66E62B19178EF9DDF05C4F
SHA1:	91A1B33403F6298C0B08FBF3FFC9A0B0B1E17D3E
SHA-256:	2BBDDFE485FC1D6A2199AD0842D025D3CFA287567C03F0048E2AC501C1C56B34
SHA-512:	691F4496ECE1946CB1B686873B5BBDB39AFAD5CB138CA713E2FA73D01850A8C2C0C1805CBFC5EA2B77BE708E061A9F6ADDC9731419A5EA6112134EF5270E2E42
Malicious:	false
Reputation:	unknown
Preview:	2025/01/07-09:59:18.615 1b68 Creating DB C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Local Storage\leveldb since it was missing..2025/01/07-09:59:18.715 1b68 Reusing MANIFEST C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Local Storage\leveldb/MANIFEST-000001.

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Login Data

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 21, cookie 0xc, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	43008
Entropy (8bit):	0.9009435143901008
Encrypted:	false
SSDEEP:	
MD5:	FB3D677576C25FF04A308A1F627410B7
SHA1:	97D530911F9CB0C37717ABB145D748982ADA0440

SHA-256:	A79300470D18AF26E3C5B4F23F81915B92D490105CE84A8122BF8100EC0C7517
SHA-512:	ED6666B064958B107E55BD76E52D2E5BF7A4791379902D208EF909A6B68803240D372CE03641249EB917C241B36A5684656A48D099A8A084AD34BA009857B098
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Network Action Predictor

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 3, database pages 11, cookie 0x6, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	0.40293591932113104
Encrypted:	false
SSDEEP:	
MD5:	ADC0CFB8A1A20DE2C4AB738B413CBEA4
SHA1:	238EF489E5FDC6EBB36F09D415FB353350E7097B
SHA-256:	7C071E36A64FB1881258712C9880F155D9CBAC693BADCC391A1CB110C257CC37
SHA-512:	38C8B7293B8F7BEF03299BAFB981EEEE309945B1BDE26ACDAD6FDD63247C21CA04D493A1DDAFC3B9A1904EFED998E9C7C0C8E98506FD4AC0AB252DFF34566B66
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....j.....=.....\.t.+.>..,...=..... ....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Network\18bb1f98-87d8-466d-965f-54c5dc3ed76c.tmp

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	
MD5:	D751713988987E9331980363E24189CE
SHA1:	97D170E1550EEE4AFC0AF065B78CDA302A97674C
SHA-256:	4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945
SHA-512:	B25B294CB4DEB69EA00A4C3CF3113904801B6015E5956BD019A8570B1FE1D6040E944EF3CDEE16D0A46503CA6E659A25F21CF9CEDDC13F352A3C98138C15D6AF
Malicious:	false
Reputation:	unknown
Preview:	[]

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Network\3de814c9-f32c-4d27-82b4-8fc2cd20a79e.tmp

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	59
Entropy (8bit):	4.619434150836742
Encrypted:	false
SSDEEP:	
MD5:	2800881C775077E1C4B6E06BF4676DE4
SHA1:	2873631068C8B3B9495638C865915BE822442C8B
SHA-256:	226EEC4486509917AA336AFEBD6FF65777B75B65F1FB06891D2A857A9421A974
SHA-512:	E342407AB65CC68F1B3FD706CD0A37680A0864FFD30A6539730180EDE2CDCD732CC97AE0B9EF7DB12DA5C0F83E429DF0840DBF7596ACA859A0301665E51737B
Malicious:	false
Reputation:	unknown

Preview:	{"net":{"network_qualities":{"CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Network\6c6aac3d-6754-4750-8b55-6bced6676fb2.tmp

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	111
Entropy (8bit):	4.718418993774295
Encrypted:	false
SSDEEP:	
MD5:	285252A2F6327D41EAB203DC2F402C67
SHA1:	ACEDB7BA5FBC3CE914A8BF386A6F72CA7BAA33C6
SHA-256:	5DFC321417FC31359F23320EA68014EBFD793C5BBED55F77DAB4180BBD4A2026
SHA-512:	11CE7CB484FEE66894E63C31DB0D6B7EF66AD0327D4E7E2EB85F3BCC2E836A3A522C68D681E84542E471E54F765E091EFE1EE4065641B0299B15613EB32DCC0D
Malicious:	false
Reputation:	unknown
Preview:	{"net":{"http_server_properties":{"servers":[],"version":5},"network_qualities":{"CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Network\Cookies

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 7, database pages 5, cookie 0x5, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6732424250451717
Encrypted:	false
SSDEEP:	
MD5:	CFFF4E2B77FC5A18AB6323AF9BF95339
SHA1:	3AA2C2115A8EB4516049600E8832E9BFFE0C2412
SHA-256:	EC8B67EF7331A87086A6CC085B085A6B7FFFD325E1B3C90BD3B9B1B119F696AE
SHA-512:	0BFDC8D28D09558AA97F4235728AD656FE9F6F2C61DDA2D09B416F89AB60038537B7513B070B907E57032A68B9717F03575DB6778B68386254C8157559A3F1BC
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....j...$.....g..... ....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Network\Network Persistent State (copy)

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	
MD5:	2800881C775077E1C4B6E06BF4676DE4
SHA1:	2873631068C8B3B9495638C865915BE822442C8B
SHA-256:	226EEC4486509917AA336AFEBD6FF65777B75B65F1FB06891D2A857A9421A974
SHA-512:	E342407AB65CC68F1B3FD706CD0A37680A0864FFD30A6539730180EDE2CDCD732CC97AE0B9EF7DB12DA5C0F83E429DF0840DBF7596ACA859A0301665E51737B
Malicious:	false
Reputation:	unknown
Preview:	{"net":{"network_qualities":{"CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Network\Network Persistent State~RF4bad2b.TMP (copy)

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	JSON data
Category:	dropped

Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	
MD5:	2800881C775077E1C4B6E06BF4676DE4
SHA1:	2873631068C8B3B9495638C865915BE822442C8B
SHA-256:	226EEC4486509917AA336AFEBD6FF65777B75B65F1FB06891D2A857A9421A974
SHA-512:	E342407AB65CC68F1B3FD706CD0A37680A0864FFD30A6539730180EDE2CDCD732CC97AE0B9EF7DB12DA5C0F83E429DF0840DBF7596ACA859A0301665E51737B
Malicious:	false
Reputation:	unknown
Preview:	{"net":{"network_qualities":{"CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Network\Reporting and NEL

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 4, database pages 9, cookie 0x4, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	36864
Entropy (8bit):	0.5559635235158827
Encrypted:	false
SSDEEP:	
MD5:	9AAAE8C040B616D1378F3E0E17689A29
SHA1:	F91E7DE07F1DA14D15D067E1F50C3B84A328DBB7
SHA-256:	5B94D63C31AE795661F69B9D10E8BFD115584CD6FEF5FBB7AA483FDC6A66945B
SHA-512:	436202AB8B6BB0318A30946108E6722DFF781F462EE05980C14F57F347EDDCF8119E236C3290B580CEF6902E1B59FB4F546D6BD69F62479805B39AB0F3308EC1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....j.....g...D.....7..... ....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Network\SCT Auditing Pending Reports (copy)

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	
MD5:	D751713988987E9331980363E24189CE
SHA1:	97D170E1550EEE4AFC0AF065B78CDA302A97674C
SHA-256:	4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945
SHA-512:	B25B294CB4DEB69EA00A4C3CF3113904801B6015E5956BD019A8570B1FE1D6040E944EF3CDEE16D0A46503CA6E659A25F21CF9CEDDC13F352A3C98138C15D6AF
Malicious:	false
Reputation:	unknown
Preview:	[]

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Network\SCT Auditing Pending Reports~RF4a841c.TMP (copy)

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	
MD5:	D751713988987E9331980363E24189CE
SHA1:	97D170E1550EEE4AFC0AF065B78CDA302A97674C
SHA-256:	4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945

SHA-512:	B25B294CB4DEB69EA00A4C3CF3113904801B6015E5956BD019A8570B1FE1D6040E944EF3CDEE16D0A46503CA6E659A25F21CF9CEDDC13F352A3C98138C15D6AF
Malicious:	false
Reputation:	unknown
Preview:	[]

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Network\Sdch Dictionaries (copy)

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	
MD5:	20D4B8FA017A12A108C87F540836E250
SHA1:	1AC617FAC131262B6D3CE1F52F5907E31D5F6F00
SHA-256:	6028BD681DBF11A0A58DDE8A0CD884115C04CAA59D080BA51BDE1B086CE0079D
SHA-512:	507B2B8A8A168FF8F2BDAFA5D9D341C44501A5F17D9F63F3D43BD586BC9E8AE33221887869FA86F845B7D067CB7D2A7009EFD71DDA36E03A40A74FEE04B8686
Malicious:	false
Reputation:	unknown
Preview:	{"SDCH":{"dictionaries":{},"version":2}}

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Network\Trust Tokens

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 3, database pages 9, cookie 0x6, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	36864
Entropy (8bit):	0.36515621748816035
Encrypted:	false
SSDEEP:	
MD5:	25363ADC3C9D98BAD1A33D0792405CBF
SHA1:	D06E343087D86EF1A06F7479D81B26C90A60B5C3
SHA-256:	6E019B8B9E389216D5BDF1F2FE63F41EF98E71DA101F2A6BE04F41CC5954532D
SHA-512:	CF7EEE35D0E00945AF221BEC531E8BF06C08880DA00BD103FA561BC069D7C6F955CBA3C1C152A4884601E5A670B7487D39B4AE9A4D554ED8C14F129A74E555F7
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....j.....X..g...}.....$.X..... ....

C:\Users\user\AppData\Local\Temp\MSSPWebEB\EBWebView\Default\Network\da1f83ab-0a1d-4413-9bc1-e41d02be74c7.tmp

Process:	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\117.0.2045.47\msedgewebview2.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	4.1275671571169275
Encrypted:	false
SSDEEP:	
MD5:	20D4B8FA017A12A108C87F540836E250
SHA1:	1AC617FAC131262B6D3CE1F52F5907E31D5F6F00
SHA-256:	6028BD681DBF11A0A58DDE8A0CD884115C04CAA59D080BA51BDE1B086CE0079D
SHA-512:	507B2B8A8A168FF8F2BDAFA5D9D341C44501A5F17D9F63F3D43BD586BC9E8AE33221887869FA86F845B7D067CB7D2A7009EFD71DDA36E03A40A74FEE04B8686
Malicious:	false
Reputation:	unknown
Preview:	{"SDCH":{"dictionaries":{},"version":2}}

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.999358916418884
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecurityScan_Release.exe
File size:	27'660'968 bytes
MD5:	d19f7fb266813e0fba1d009be48c40d5
SHA1:	49ad30dc2a86fb3f3f21aeeefd79bce2c9f9ef82
SHA256:	9b6d586380337296d53a605b487b442e0a32b857cccdf153c602bd1438413261
SHA512:	a3277d635573bc7d45818a91bc6d1080439e83fb700486efc74dfb1fe6a1d97811e9c6cd4f158d083abc8ca8e5c4e3b703f3ce249069b69aace0c028fc1ce5dc
SSDEEP:	786432:2fWTg0k4wDw5NQNdJO6gwQNajcQQ1xZWq2b5hWsxFe:3zgw4wwYaoTTWqw7U
TLSH:	B457332C41812B4AD739C43D6F46F0EDCB7E7EF77A40B5AA6F2807447B699821C8168D
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... (...F...F...F.*.....F...G.v.F.*.....F...v...F...@...F.Rich..F.....PE..L... ..\.....b.....

File Icon

Icon Hash:	f0b34d6961f0130f

Static PE Info

General

Entrypoint:	0x403328
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x5C157F20 [Sat Dec 15 22:24:32 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	57e98d9a5a72c8d7ad8fb7a6a58b3daf

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=GlobalSign GCC R45 EV CodeSigning CA 2020, O=GlobalSign nv-sa, C=BE
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 13/10/2023 16:08:48 13/10/2026 16:08:48
Subject Chain	• CN="McAfee, LLC", O="McAfee, LLC", STREET=6220 America Ctr Dr, L=San Jose, S=California, C=US, OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, SERIALNUMBER=2306741, OID.2.5.4.15=Private Organization
Version:	3
Thumbprint MD5:	B3515A8A7E95C305ACE3094E13C5AB18
Thumbprint SHA-1:	AAFB69C1A3FD4C2D5207E98F818B994664DB71CD
Thumbprint SHA-256:	E310C8CE8BDB286B22EFAD3B0FEC70867B7A888200331004C19DB3687CA9F170
Serial:	47E0D8578AB200083919FA11

Entrypoint Preview
Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A130h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080A8h]
call dword ptr [004080A4h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042472Ch], eax
je 00007F3A690016F3h
push ebx
call 00007F3A690047E2h
cmp eax, ebx
je 00007F3A690016E9h
push 00000C00h
call eax
mov esi, 00408298h
push esi
call 00007F3A6900475Eh
push esi
call dword ptr [004080A0h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F3A690016CDh
push 0000000Ah
call 00007F3A690047B6h
push 00000008h
call 00007F3A690047AFh
push 00000006h
mov dword ptr [00424724h], eax
call 00007F3A690047A3h
cmp eax, ebx
je 00007F3A690016F1h
push 0000001Eh
call eax
test eax, eax
je 00007F3A690016E9h
or byte ptr [0042472Fh], 00000040h
push ebp
call dword ptr [00408044h]
push ebx
call dword ptr [00408288h]
mov dword ptr [004247F8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0041FCF0h
call dword ptr [00408178h]
push 0040A1ECh

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8430	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3a000	0x19e28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x1a5e380	0x2f28	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x298	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6077	0x6200	0311bcb2ead177b380555800a8e6e6ee	False	0.6595583545918368	data	6.403859519216241	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1250	0x1400	926b1e688f085d737343e22bcf628243	False	0.4298828125	data	5.044807654453153	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x1a838	0x400	9b72314b8d9ad5c72778b00cdf336ee2	False	0.646484375	data	5.2244513108529995	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x25000	0x15000	0x0	d41d8cd98f00b204e9800998ecf8427e	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3a000	0x19e28	0x1a000	c192cd761a2f8b017781fd898ee0eaeb	False	0.17032564603365385	data	4.017066897842131	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_ICON	0x3a5f8	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 67584	English	United States	0.056089554004495445
RT_ICON	0x4ae20	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States	0.14107883817427386
RT_ICON	0x4d3c8	0x1b6e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States	0.9115636570777557
RT_ICON	0x4ef38	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States	0.21904315196998123
RT_ICON	0x4ffe0	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2688	English	United States	0.3734008528784648
RT_ICON	0x50e88	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1152	English	United States	0.4918772563176895
RT_ICON	0x51730	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1536	English	United States	0.38353658536585367
RT_ICON	0x51d98	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 320	English	United States	0.6098265895953757
RT_ICON	0x52300	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States	0.43882978723404253

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_ICON	0x52768	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	English	United States	0.4959677419354839
RT_ICON	0x52a50	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192	English	United States	0.6013513513513513
RT_DIALOG	0x52b78	0x100	data	English	United States	0.5234375
RT_DIALOG	0x52c78	0x11c	data	English	United States	0.6056338028169014
RT_DIALOG	0x52d98	0x60	data	English	United States	0.7291666666666666
RT_DIALOG	0x52df8	0xf8	data	English	United States	0.532258064516129
RT_DIALOG	0x52ef0	0x114	data	English	United States	0.6376811594202898
RT_DIALOG	0x53008	0x58	data	English	United States	0.7840909090909091
RT_DIALOG	0x53060	0xec	data	English	United States	0.5042372881355932
RT_DIALOG	0x53150	0x108	data	English	United States	0.6212121212121212
RT_DIALOG	0x53258	0x4c	data	English	United States	0.75
RT_DIALOG	0x532a8	0xec	data	English	United States	0.5042372881355932
RT_DIALOG	0x53398	0x108	data	English	United States	0.6136363636363636
RT_DIALOG	0x534a0	0x4c	data	English	United States	0.75
RT_DIALOG	0x534f0	0xf0	data	English	United States	0.5125
RT_DIALOG	0x535e0	0x10c	data	English	United States	0.6343283582089553
RT_DIALOG	0x536f0	0x50	data	English	United States	0.7625
RT_GROUP_ICON	0x53740	0xa0	data	English	United States	0.63125
RT_VERSION	0x537e0	0x2f4	data	Chinese	Taiwan	0.45634920634920634
RT_MANIFEST	0x53ad8	0x349	XML 1.0 document, ASCII text, with very long lines (841), with no line terminators	English	United States	0.5517241379310345

Imports

DLL	Import
KERNEL32.dll	SetEnvironmentVariableA, CreateFileA, GetFileSize, GetModuleFileNameA, ReadFile, GetCurrentProcess, CopyFileA, Sleep, GetTickCount, GetWindowsDirectoryA, GetTempPathA, GetCommandLineA, lstrlenA, GetVersion, SetErrorMode, lstrcpynA, ExitProcess, SetCurrentDirectoryA, GlobalLock, CreateThread, GetLastError, CreateDirectoryA, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, WriteFile, lstrcpyA, MoveFileExA, lstrcatA, GetSystemDirectoryA, GetProcAddress, GetExitCodeProcess, WaitForSingleObject, CompareFileTime, SetFileAttributesA, GetFileAttributesA, GetShortPathNameA, MoveFileA, GetFullPathNameA, SetFileTime, SearchPathA, CloseHandle, lstrcmpiA, GlobalUnlock, GetDiskFreeSpaceA, lstrcmpA, FindFirstFileA, FindNextFileA, DeleteFileA, SetFilePointer, GetPrivateProfileStringA, FindClose, MultiByteToWideChar, FreeLibrary, MulDiv, WritePrivateProfileStringA, LoadLibraryExA, GetModuleHandleA, GlobalAlloc, GlobalFree, ExpandEnvironmentStringsA
USER32.dll	ScreenToClient, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, PostQuitMessage, GetWindowRect, EnableMenuItem, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, ReleaseDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndDialog, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, GetDC, CreateDialogParamA, SetTimer, GetDlgItem, SetWindowLongA, SetForegroundWindow, LoadImageA, IsWindow, SendMessageTimeoutA, FindWindowExA, OpenClipboard, TrackPopupMenu, AppendMenuA, EndPaint, DestroyWindow, wsprintfA, ShowWindow, SetWindowTextA
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectA, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, ShellExecuteExA, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, SHFileOperationA
ADVAPI32.dll	AdjustTokenPrivileges, RegCreateKeyExA, RegOpenKeyExA, SetFileSecurityA, OpenProcessToken, LookupPrivilegeValueA, RegEnumValueA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan