ID: 877863
Sample Name: CgpIx13Spu.exe
Cookbook: default.jbs
Time: 06:21:08
Date: 30/05/2023
Version: 37.1.0 Beryl

Table of Contents

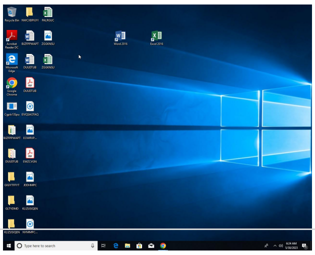
Windows Analysis Report

CgpIx13Spu.exe

Overview

General Information

Sample Name:	CgpIx13Spu.exe
Original Sample Name:	dc586fef0d44e…
Analysis ID:	877863
MD5:	dc586fef0d44e…
SHA1:	d08b8281eebd..
SHA256:	6bac4b7f411a6..
Tags:	exe NanoCore RAT
Infos:	YARA SIGMA



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

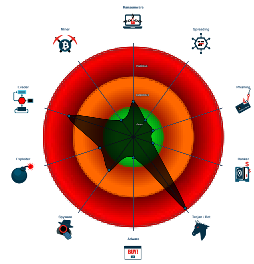
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Sigma detected: Scheduled temp fil…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- CgpIx13Spu.exe (PID: 7060 cmdline: C:\Users\user\Desktop\CgpIx13Spu.exe MD5: DC586FEF0D44E3B50964F916AB75A44F)
  - powershell.exe (PID: 1412 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\CgpIx13Spu.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5200 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4028 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3984 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 2344 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\unFmnPEZpvL" /XML "C:\Users\user\AppData\Local\Temp\tmp7EB8.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7112 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - CgpIx13Spu.exe (PID: 7456 cmdline: C:\Users\user\Desktop\CgpIx13Spu.exe MD5: DC586FEF0D44E3B50964F916AB75A44F)
- unFmnPEZpvL.exe (PID: 7336 cmdline: C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe MD5: DC586FEF0D44E3B50964F916AB75A44F)
  - schtasks.exe (PID: 7740 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\unFmnPEZpvL" /XML "C:\Users\user\AppData\Local\Temp\tmpB1AF.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7748 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - unFmnPEZpvL.exe (PID: 7784 cmdline: C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe MD5: DC586FEF0D44E3B50964F916AB75A44F)
  - unFmnPEZpvL.exe (PID: 7792 cmdline: C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe MD5: DC586FEF0D44E3B50964F916AB75A44F)
- dhcpmon.exe (PID: 7852 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: DC586FEF0D44E3B50964F916AB75A44F)
  - schtasks.exe (PID: 7916 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\unFmnPEZpvL" /XML "C:\Users\user\AppData\Local\Temp\tmpDAE1.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 7980 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: DC586FEF0D44E3B50964F916AB75A44F)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
Nanocore RAT, NanoCore	Nanocore is a Remote Access Tool used to steal credentials and to spy on cameras. It as been used for a while by numerous criminal actors as well as by nation state threat actors.	• APT33 • The Gorgon Group	**http://** https://assets.virustotal.com/reports/2021trends.pdfhttps://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/https://blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/https://blog.morphisec.com/syk-crypter-discord	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.nanocore

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "2b192589-e692-4024-abbd-8fa6959a",
  "Group": "Airy",
  "Domain1": "atelilian99.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 9387,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "",
  "BackupDNSServer": "37.235.1.177"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.596149804.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000F.00000002.596149804.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000000F.00000002.596149804.0000000000402000.00000040.00000400.00020000.00000000.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:$j: #=q
0000000F.00000002.596149804.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xff8d:$a1: NanoCore.ClientPluginHost • 0xff4d:$a2: NanoCore.ClientPlugin • 0x11ea6:$b1: get_BuilderSettings • 0xfda9:$b2: ClientLoaderForm.resources • 0x115c6:$b3: PluginCommand • 0xff7e:$b4: IClientAppHost • 0x1a3fe:$b5: GetBlockHash • 0x124fe:$b6: AddHostEntry • 0x161f1:$b7: LogClientException • 0x1246b:$b8: PipeExists • 0xffb7:$b9: IClientLoggingHost
0000000A.00000002.812707754.0000000003C2B000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xfbb:$a1: NanoCore.ClientPluginHost • 0xf7e:$a2: NanoCore.ClientPlugin
Click to see the 51 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
19.2.dhcpmon.exe.2db9658.0.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
19.2.dhcpmon.exe.2db9658.0.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
19.2.dhcpmon.exe.2db9658.0.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xe38:$x2: NanoCore.ClientPlugin • 0xe75:$x3: NanoCore.ClientPluginHost • 0xe5a:$i1: IClientApp • 0xe4e:$i2: IClientData • 0xe29:$i3: IClientNetwork • 0xec3:$i4: IClientAppHost • 0xe65:$i5: IClientDataHost • 0xeb0:$i6: IClientLoggingHost • 0xe8f:$i7: IClientNetworkHost • 0xea2:$i8: IClientUIHost • 0xed2:$i9: IClientNameObjectCollection • 0xef7:$i10: IClientReadOnlyNameObjectCollection • 0xe41:$s1: ClientPlugin • 0x177c:$s1: ClientPlugin • 0x1789:$s1: ClientPlugin • 0x11f9:$s6: get_ClientSettings • 0x1249:$s7: get_Connected
19.2.dhcpmon.exe.2db9658.0.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xe75:$a1: NanoCore.ClientPluginHost • 0xe38:$a2: NanoCore.ClientPlugin • 0x120c:$b1: get_BuilderSettings • 0xec3:$b4: IClientAppHost • 0x127d:$b6: AddHostEntry • 0x12ec:$b7: LogClientException • 0x1261:$b8: PipeExists • 0xeb0:$b9: IClientLoggingHost
10.2.CgpIx13Spu.exe.3c2b146.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 114 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 213.152.162.181 - Destination IP: 192.168.2.4	
Timestamp:	213.152.162.181192.168.2.49387496962841753 05/30/23-06:23:12.736325
SID:	2841753
Source Port:	9387
Destination Port:	49696
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 213.152.162.181	
Timestamp:	192.168.2.4213.152.162.1814969793872025019 05/30/23-06:23:42.157295
SID:	2025019
Source Port:	49697
Destination Port:	9387
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 213.152.162.181	
Timestamp:	192.168.2.4213.152.162.1814969693872025019 05/30/23-06:23:12.265301
SID:	2025019
Source Port:	49696
Destination Port:	9387
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 213.152.162.181	
Timestamp:	192.168.2.4213.152.162.1814969593872025019 05/30/23-06:22:41.923978
SID:	2025019
Source Port:	49695
Destination Port:	9387
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 213.152.162.181	
Timestamp:	192.168.2.4213.152.162.1814969593872816766 05/30/23-06:22:42.804651
SID:	2816766

Source Port:	49695
Destination Port:	9387
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 213.152.162.181	
Timestamp:	192.168.2.4213.152.162.1814969793872816766 05/30/23-06:23:43.464776
SID:	2816766
Source Port:	49697
Destination Port:	9387
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 213.152.162.181 - Destination IP: 192.168.2.4	
Timestamp:	213.152.162.181192.168.2.49387496952841753 05/30/23-06:22:43.336347
SID:	2841753
Source Port:	9387
Destination Port:	49695
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Yara detected Nanocore RAT
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Networking

- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware configuration
- Uses dynamic DNS services

E-Banking Fraud

- Yara detected Nanocore RAT

System Summary

- Malicious sample detected (through community Yara rule)

Data Obfuscation

- .NET source code contains potential unpacker

Boot Survival

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)

HIPS / PFW / Operating System Protection Evasion

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

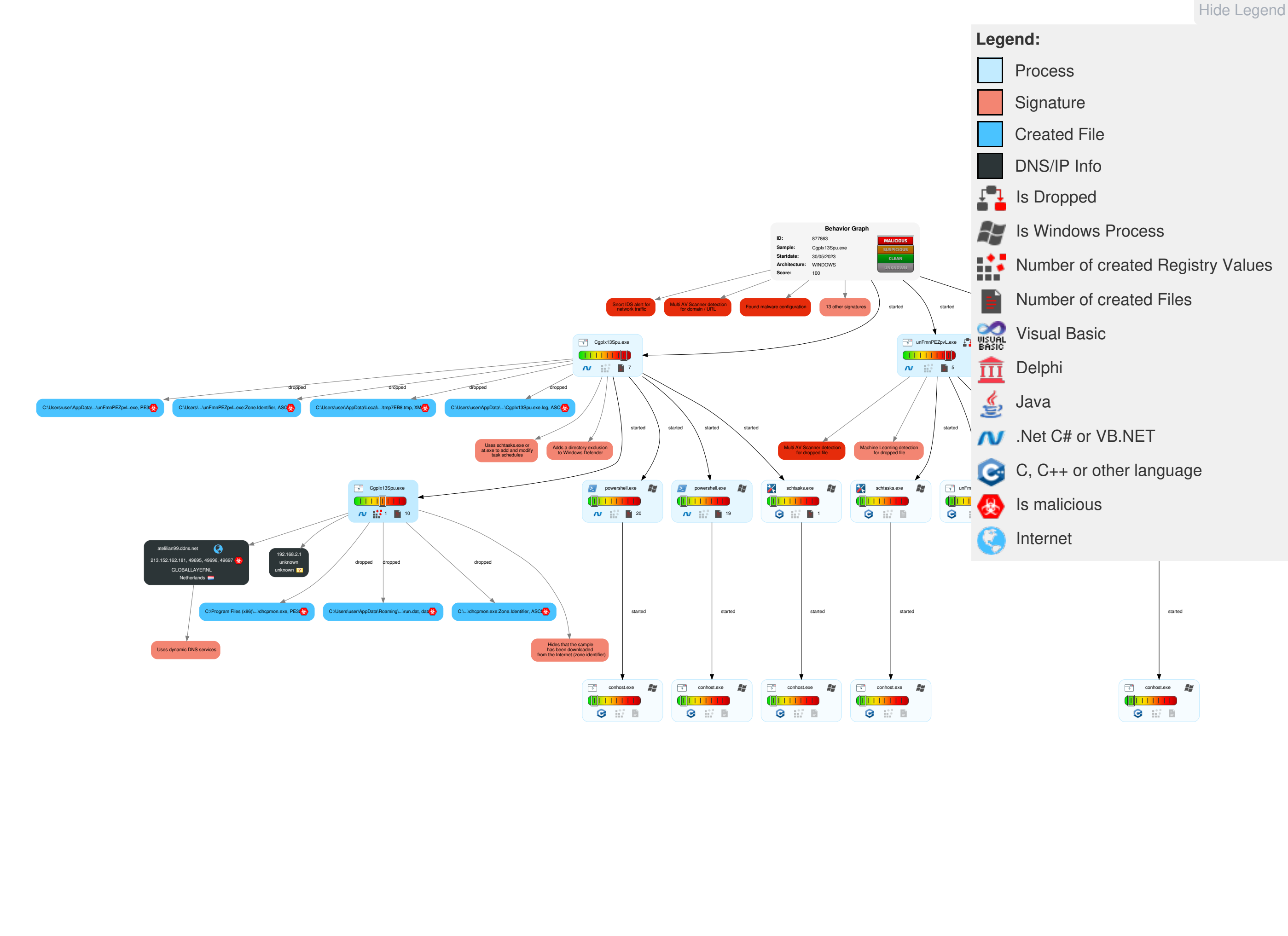
Detected Nanocore Rat

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
Valid Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	1 2 Process Injection	2 Masquerading	2 1 Input Capture	1 1 Security Software Discovery	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Obfuscated Files or Information	DCSync	1 2 System Information 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 2 Software Packing	Proc Filesystem	Network Service Scanning	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 Timestomp	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

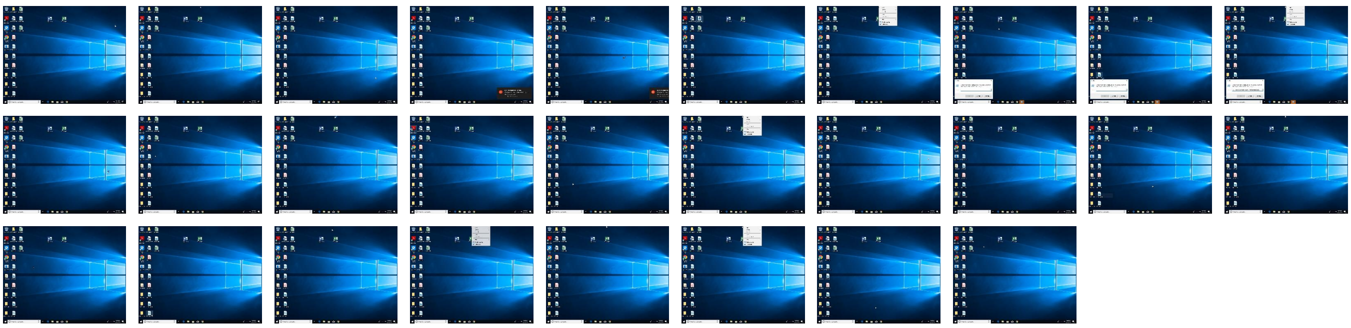
Behavior Graph



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
Cgplx13Spu.exe	65%	ReversingLabs	ByteCode-MSIL.Trojan.Agent Tesla	
Cgplx13Spu.exe	54%	Virustotal		Browse
Cgplx13Spu.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	65%	ReversingLabs	ByteCode-MSIL.Trojan.Agent Tesla	
C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe	65%	ReversingLabs	ByteCode-MSIL.Trojan.Agent Tesla	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
atelilian99.ddns.net	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/5	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/5	0%	URL Reputation	safe	
http://www.carterandcone.comD	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.carterandcone.comQ	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/h	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/U	0%	URL Reputation	safe	
http://www.tiro.comx	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Q	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/r	0%	URL Reputation	safe	
http://www.fontbureau.comlic	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalics	0%	Avira URL Cloud	safe	
http://www.fontbureau.comttF	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalicy	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/y	0%	URL Reputation	safe	
127.0.0.1	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/y	0%	URL Reputation	safe	
http://www.fontbureau.comk	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/r	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/h	0%	URL Reputation	safe	
http://www.fontbureau.commX	0%	Avira URL Cloud	safe	
http://www.fontbureau.com.TTFQ	0%	Avira URL Cloud	safe	
atelilian99.ddns.net	100%	Avira URL Cloud	malware	
http://www.sakkal.com$$	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomt	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdy	0%	Avira URL Cloud	safe	
http://www.tiro.com$$	0%	Avira URL Cloud	safe	
http://www.tiro.comen-u	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
atelilian99.ddns.net	213.152.162.181	true	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
127.0.0.1	true	• Avira URL Cloud: safe	unknown
atelilian99.ddns.net	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comalicy	CgpIx13Spu.exe, 00000000.00000003.538575060.0000000005026000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comalics	CgpIx13Spu.exe, 00000000.00000003.538575060.0000000005026000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/5	CgpIx13Spu.exe, 00000000.00000003.537917015.0000000005026000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	CgpIx13Spu.exe, 00000000.00000003.537483917.0000000005026000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comttF	CgpIx13Spu.exe, 00000000.00000003.538575060.0000000005026000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp, CgpIx13Spu.exe, 00000000.00000003.535187593.000000000502B000.00000004.00000020.00020000.00000000.sdmp, CgpIx13Spu.exe, 00000000.00000003.535170566.000000000502B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/5	CgpIx13Spu.exe, 00000000.00000003.538025853.0000000005020000.00000004.00000020.00020000.00000000.sdmp, CgpIx13Spu.exe, 00000000.00000003.538199722.0000000005026000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comD	CgpIx13Spu.exe, 00000000.00000003.537483917.0000000005026000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/4	CgpIx13Spu.exe, 00000000.00000003.537796025.000000000501B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//	CgpIx13Spu.exe, 00000000.00000003.537917015.0000000005026000.00000004.00000020.00020000.00000000.sdmp, CgpIx13Spu.exe, 00000000.00000003.537796025.000000000501B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/rep	CgpIx13Spu.exe, 00000000.00000003.538575060.0000000005012000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/DPlease	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comQ	CgpIx13Spu.exe, 00000000.00000003.538318448.0000000005012000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/h	CgpIx13Spu.exe, 00000000.00000003.537123993.0000000005027000.00000004.00000020.00020000.00000000.sdmp, CgpIx13Spu.exe, 00000000.00000003.537095958.0000000005012000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	CgpIx13Spu.exe, 00000000.00000003.537379906.0000000005022000.00000004.00000020.00020000.00000000.sdmp, CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp, CgpIx13Spu.exe, 00000000.00000003.537307172.000000000501F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CgpIx13Spu.exe, 00000000.00000002.561804154.0000000002731000.00000004.00000800.00020000.00000000.sdmp, unFmnPEZpvL.exe, 00000009.00000002.584415545.0000000002981000.00000004.00000800.00020000.00000000.sdmp, CgpIx13Spu.exe, 0000000A.00000002.804694487.0000000002BE1000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 00000010.00000002.608708717.0000000002B31000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com=	CgpIx13Spu.exe, 00000000.00000003.560043413.0000000005010000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comalsd	CgpIx13Spu.exe, 00000000.00000003.538803257.0000000005027000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	CgpIx13Spu.exe, 00000000.00000003.538803257.0000000005027000.00000004.00000020.00020000.00000000.sdmp, CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp, CgpIx13Spu.exe, 00000000.00000003.538575060.0000000005026000.00000004.00000020.00020000.00000000.sdmp, CgpIx13Spu.exe, 00000000.00000003.538631934.0000000005026000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/U	CgpIx13Spu.exe, 00000000.00000003.538025853.0000000005020000.00000004.00000020.00020000.00000000.sdmp, CgpIx13Spu.exe, 00000000.00000003.537917015.0000000005026000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.commX	CgpIx13Spu.exe, 00000000.00000003.538803257.0000000005027000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com.TTFQ	CgpIx13Spu.exe, 00000000.00000003.538803257.0000000005027000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comx	CgpIx13Spu.exe, 00000000.00000003.537123993.0000000005022000.00000004.00000020.00020000.00000000.sdmp, CgpIx13Spu.exe, 00000000.00000003.537095958.0000000005012000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Q	CgpIx13Spu.exe, 00000000.00000003.538025853.0000000005020000.00000004.00000020.00020000.00000000.sdmp, CgpIx13Spu.exe, 00000000.00000003.538199722.0000000005026000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comdy	CgpIx13Spu.exe, 00000000.00000003.538803257.0000000005027000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com$$	CgpIx13Spu.exe, 00000000.00000003.538318448.0000000005026000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/jp/r	CgpIx13Spu.exe, 00000000.00000003.538199722.0000000005026000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comlic	CgpIx13Spu.exe, 00000000.00000003.538803257.0000000005027000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comcomt	CgpIx13Spu.exe, 00000000.00000003.538803257.0000000005027000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	CgpIx13Spu.exe, 00000000.00000003.538318448.0000000005026000.00000004.00000020.00020000.00000000.sdmp, CgpIx13Spu.exe, 00000000.00000003.538025853.0000000005020000.00000004.00000020.00020000.00000000.sdmp, CgpIx13Spu.exe, 00000000.00000003.538199722.0000000005026000.00000004.00000020.00020000.00000000.sdmp, CgpIx13Spu.exe, 00000000.00000003.537917015.0000000005026000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	CgpIx13Spu.exe, 00000000.00000003.560043413.0000000005010000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	CgpIx13Spu.exe, 00000000.00000003.538803257.0000000005027000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/y	CgpIx13Spu.exe, 00000000.00000003.538199722.0000000005026000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com$$	CgpIx13Spu.exe, 00000000.00000003.537483917.0000000005026000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/y	CgpIx13Spu.exe, 00000000.00000003.538025853.0000000005020000.00000004.00000020.00020000.00000000.sdmp, CgpIx13Spu.exe, 00000000.00000003.537917015.0000000005026000.00000004.00000020.00020000.00000000.sdmp, CgpIx13Spu.exe, 00000000.00000003.537796025.000000000501B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comk	CgpIx13Spu.exe, 00000000.00000003.538575060.0000000005026000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	CgpIx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-user.html	Cgplx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y0/	Cgplx13Spu.exe, 00000000.00000003.538025853.0000000005020000.00000004.00000020.00020000.00000000.sdmp, Cgplx13Spu.exe, 00000000.00000003.538199722.0000000005026000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/r	Cgplx13Spu.exe, 00000000.00000003.538025853.0000000005020000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	Cgplx13Spu.exe, 00000000.00000003.537917015.0000000005026000.00000004.00000020.00020000.00000000.sdmp, Cgplx13Spu.exe, 00000000.00000003.537796025.000000000501B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Cgplx13Spu.exe, 00000000.00000002.571214309.00000000066A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/h	Cgplx13Spu.exe, 00000000.00000003.538025853.0000000005020000.00000004.00000020.00020000.00000000.sdmp, Cgplx13Spu.exe, 00000000.00000003.538199722.0000000005026000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comen-u	Cgplx13Spu.exe, 00000000.00000003.537123993.0000000005022000.00000004.00000020.00020000.00000000.sdmp, Cgplx13Spu.exe, 00000000.00000003.537095958.0000000005012000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
213.152.162.181	atelilian99.ddns.net	Netherlands		49453	GLOBALLAYERNL	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	877863
Start date and time:	2023-05-30 06:21:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
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
Sample file name:	CgpIx13Spu.exe
Original Sample Name:	dc586fef0d44e3b50964f916ab75a44f.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@26/17@43/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, WMIADAP.exe, WmiPrvSE.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior 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 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
06:22:03	API Interceptor	939x Sleep call for process: CgpIx13Spu.exe modified
06:22:07	Task Scheduler	Run new task: unFmnPEZpvL path: C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe
06:22:07	API Interceptor	65x Sleep call for process: powershell.exe modified
06:22:13	API Interceptor	1x Sleep call for process: unFmnPEZpvL.exe modified
06:22:17	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
06:22:28	API Interceptor	1x Sleep call for process: dhcpmon.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\CgpIx13Spu.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	696320
Entropy (8bit):	7.758655688397579
Encrypted:	false
SSDEEP:	12288:e2N8jiZ4zypIPsKtPplTY6RhKuYqwxCWeWNsx0+Mzhe4rJQzSINgh2cywOuZq7Ie:e2N8jiZ4zypIPsKJTDEqACUlhe4rJTX6
MD5:	DC586FEF0D44E3B50964F916AB75A44F
SHA1:	D08B8281EEBD2221521C333BDBB5D74AA8A92D0A
SHA-256:	6BAC4B7F411A6895A9992B4DDCE92D251DFE63C4AAFAB668D0C525DE4EDDD5F2
SHA-512:	2991BE29DCB33C7E50C40D36CBD116D22BC3846ED8283956B7096BD5F76998D250F2A5DF40D99CFEFD18BE6D0A5BAB1CE4D1C56E286C263E87DFABCBF6AE C87F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 65%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....................0.............r.... ....@.. ....@................................ ...O..................................H...p.. ....H............text...x.... ....`.rsrc..............................@..@.rel oc..............................@..B................T.......H.......@....[......a.......X..^..}.....(.......(.....*...{.....o......{.....o......{.....o......(.....*....0...........r...p...(n...}.....{..... {....o......{....o.....o....r-..po......{....o.....o....r=..po......{....o.....o....rO..po......{....o.....o....ra..po......{....o.....o....rq..po......{....o.....o....ry..po......{....o.....o.....Po......{....o.....o.... .. ..o......{....o.....o.....Po......{....o.....o.....do......{....o.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\CgpIx13Spu.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E

Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CgpIx13Spu.exe.log

Process:	C:\Users\user\Desktop\CgpIx13Spu.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1302
Entropy (8bit):	5.3499841584777394
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84bE4Ks:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	4664C2114894A4BFC1E657FC08C72FF4
SHA1:	95A1E14E2AD65BCA561261DA3899074BF5276AED
SHA-256:	6E36229D13672B4304C696812B365F2E5657875DD0E11F13AE010566CC87607A
SHA-512:	4E7862716D5C0BC2174E819BAB329A2974FE83A36D5417EE732AB2F3D77D95620B3D462A1C9608F5FE90A48030140DE53DB642F8C370CD8E191BDBE83C638C 1
Malicious:	**true**
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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\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\S ystem.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b 77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_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):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178 FF6
Malicious:	false
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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\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\S ystem.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b 77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\unFmnPEZpvL.exe.log

Process:	C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178 FF6
Malicious:	false

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\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	21896
Entropy (8bit):	5.595076717117252
Encrypted:	false
SSDEEP:	384:bQtCR7q09Q5cPxBn3wOYSBxnujulrItGiJ9g5SJ3uyV1Jm021AVrdAkY0A+iSYb:bw+PdY4xuClrSm5cuCX+b
MD5:	02D4F39296832B3BA6DAFCD848D4C7C8
SHA1:	3B380E1A9EE6548379DADFF26046C62440855F8E
SHA-256:	13C2C9F9A79D5ADFCEEF862EB65DD62B1811ACC9D03151CEE2045992D8B1F1AE
SHA-512:	F704279DD2875DB9120CF9135D93659F7C94E2798F897A7B892D713BE995D24B9119B319994F56BD27C95F952A82831B2E08EB946F39484C0E6865C509BF2A83
Malicious:	false
Preview:	@...e...............................(................@..........H...............<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD...............fZve...F.....x.)........System.Management.Automation4...............[...{a.C..%6..h.........System.Core.0...............G-.o...A...4B..........System..4................Zg5..:O..g..q..........System.Xml..L...............7.....J@......~.......#.Microsoft.Management.Infrastructure.8................'....L..}............System.Numerics.@...............Lo...QN......<Q........System.DirectoryServices<................H..QN.Y.f............System.Management...4....................].D.E.....#.......System.Data.H................. ....H..m)aUu.........Microsoft.PowerShell.Security...<.................~.[L.D.Z.>..m.........System.Transactions.<................):gK..G...$.1.q........System.ConfigurationP................/.C..J..%...]......%.Microsoft.PowerShell.Commands.Utility...D.................-.D.F.<;.nt.1........System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2vfoed4z.egy.ps1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_etowe3li.cjh.ps1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_r4xwpnyv.mvb.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xc2sbisk.3fp.psm1

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

C:\Users\user\AppData\Local\Temp\tmp7EB8.tmp

Process:	C:\Users\user\Desktop\CgpIx13Spu.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1598
Entropy (8bit):	5.140726940577047
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtaExvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTbv
MD5:	70E4C0E48F210D390D9BC0D2AD175770
SHA1:	8B77A9E3693E06E70165AB847C5D1DF821E1D015
SHA-256:	19FEEE7B05F20D2D2BB60E224CCDC0D2EB3343811233C996C00893AF5D1C2812
SHA-512:	C4CF2E759CE1DFA5C9765D2F9952BD64B726674F5FC4571F91A6D9EC74C87E459863BFE95A74354784119F16ED6C00180F7D06D44A1C4B012DF6AAF234B2BE2
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Local\Temp\tmpB1AF.tmp

Process:	C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1598
Entropy (8bit):	5.140726940577047
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtaExvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTbv
MD5:	70E4C0E48F210D390D9BC0D2AD175770
SHA1:	8B77A9E3693E06E70165AB847C5D1DF821E1D015
SHA-256:	19FEEE7B05F20D2D2BB60E224CCDC0D2EB3343811233C996C00893AF5D1C2812

SHA-512:	C4CF2E759CE1DFA5C9765D2F9952BD64B726674F5FC4571F91A6D9EC74C87E459863BFE95A74354784119F16ED6C00180F7D06D44A1C4B012DF6AAF234B2BE2
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Local\Temp\tmpDAE1.tmp

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1598
Entropy (8bit):	5.140726940577047
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtaExvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTbv
MD5:	70E4C0E48F210D390D9BC0D2AD175770
SHA1:	8B77A9E3693E06E70165AB847C5D1DF821E1D015
SHA-256:	19FEEE7B05F20D2D2BB60E224CCDC0D2EB3343811233C996C00893AF5D1C2812
SHA-512:	C4CF2E759CE1DFA5C9765D2F9952BD64B726674F5FC4571F91A6D9EC74C87E459863BFE95A74354784119F16ED6C00180F7D06D44A1C4B012DF6AAF234B2BE2
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

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

Process:	C:\Users\user\Desktop\CgpIx13Spu.exe
File Type:	data
Category:	modified
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35 A5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.....@.3..{...grv+V...B.......].P...W.4C}uL.....s~..F...}......E......E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

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

Process:	C:\Users\user\Desktop\CgpIx13Spu.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:YwEt:g
MD5:	C59B0B18C8475E4D66705A4A34FD91CC
SHA1:	E8398A8A8A6E4571DA88382D478E7021F567CDC4
SHA-256:	ECDDA12382ECCDB28601D1673E99A2E640563D92F2F40DB4A76B7A00EBA77B93
SHA-512:	A2BA3660F18E0D9BC1E96E11A9A35CDAF8E172C0811EBD4E227E9EBEF48E3FF92BF8B37B4C52768192351CD721FF144103ED8111F0859D722F2EE37BB93D3E C
Malicious:	**true**
Preview:	5..r.`.H

C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe	
Process:	C:\Users\user\Desktop\CgpIx13Spu.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	696320
Entropy (8bit):	7.758655688397579
Encrypted:	false
SSDEEP:	12288:e2N8jiZ4zypIPsKtPpITY6RhKuYqwxCWeWNsx0+Mzhe4rJQzSINgh2cywOuZq7Ie:e2N8jiZ4zypIPsKJTDEqACUlhe4rJTX6
MD5:	DC586FEF0D44E3B50964F916AB75A44F
SHA1:	D08B8281EEBD2221521C333BDBB5D74AA8A92D0A
SHA-256:	6BAC4B7F411A6895A9992B4DDCE92D251DFE63C4AAFAB668D0C525DE4EDDD5F2
SHA-512:	2991BE29DCB33C7E50C40D36CBD116D22BC3846ED8283956B7096BD5F76998D250F2A5DF40D99CFEFD18BE6D0A5BAB1CE4D1C56E286C263E87DFABCBF6AEC87F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 65%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....................0.............r.... ....@.. ....@................................ ...O..................................H...p... ....H............text...x.... ....`.rsrc..............................@..@.rel oc..............................@..B................T.......H.......@....[......a.......X..^..}.....(.......(.....*...{.....o......{.....o......{.....o......(.....*....0...........r...p...(n...}.....{.....{....o......{....o.....o....r-..po......{....o.....o....r=..po......{....o.....o....rO..po......{....o.....o....ra..po......{....o.....o....rq..po......{....o.....o....ry..po......{....o.....o.....Po......{....o.....o.... .. ..o......{....o.....o.....Po......{....o.....o.....do......{....o.....

C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\CgpIx13Spu.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**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.758655688397579
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% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	CgpIx13Spu.exe
File size:	696320
MD5:	dc586fef0d44e3b50964f916ab75a44f
SHA1:	d08b8281eebd2221521c333bdbb5d74aa8a92d0a
SHA256:	6bac4b7f411a6895a9992b4ddce92d251dfe63c4aafab668d0c525de4eddd5f2
SHA512:	2991be29dcb33c7e50c40d36cbd116d22bc3846ed8283956b7096bd5f76998d250f2a5df40d99cfefd18be6d0a5bab1ce4d1c56e286c263e87dfabcbf6aec87f
SSDEEP:	12288:e2N8jiZ4zypIPsKtPpITY6RhKuYqwxCWeWNsx0+Mzhe4rJQzSINgh2cywOuZq7Ie:e2N8jiZ4zypIPsKJTDEqACUlhe4rJTX6
TLSH:	D8E402C43379AF46D873A7F4445452B8437EA86AB932E3430D83F0DA9AA5F444E91F1B
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....................0.............r.... ....@.. ....@................................

File Icon

Icon Hash:	90cecececе8e8eb0

Static PE Info

General

Entrypoint:	0x4ab472
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xFB9F168F [Thu Oct 11 00:53:35 2103 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xab420	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xac000	0x5ac	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xae000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xa9448	0x70	.text
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	0xa9478	0xa9600	False	0.9084986162361623	data	7.76575096360064	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xac000	0x5ac	0x600	False	0.421875	data	4.087184081731354	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xae000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xac090	0x31c	data		
RT_MANIFEST	0xac3bc	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
213.152.162.181192.168.2.49387496962841753 05/30/23-06:23:12.736325	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	9387	49696	213.152.162.181	192.168.2.4
192.168.2.4213.152.162.1814969793872025019 05/30/23-06:23:42.157295	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49697	9387	192.168.2.4	213.152.162.181
192.168.2.4213.152.162.1814969693872025019 05/30/23-06:23:12.265301	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49696	9387	192.168.2.4	213.152.162.181
192.168.2.4213.152.162.1814969593872025019 05/30/23-06:22:41.923978	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49695	9387	192.168.2.4	213.152.162.181
192.168.2.4213.152.162.1814969593872816766 05/30/23-06:22:42.804651	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49695	9387	192.168.2.4	213.152.162.181
192.168.2.4213.152.162.1814969793872816766 05/30/23-06:23:43.464776	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49697	9387	192.168.2.4	213.152.162.181
213.152.162.181192.168.2.49387496952841753 05/30/23-06:22:43.336347	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	9387	49695	213.152.162.181	192.168.2.4

Network Port Distribution

Total Packets: 87

- 53 (DNS)
- 9387 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 30, 2023 06:22:41.508732080 CEST	49695	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:22:41.744621992 CEST	9387	49695	213.152.162.181	192.168.2.4
May 30, 2023 06:22:41.744760990 CEST	49695	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:22:41.923978090 CEST	49695	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:22:42.487500906 CEST	9387	49695	213.152.162.181	192.168.2.4
May 30, 2023 06:22:42.541939974 CEST	49695	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:22:42.613882065 CEST	49695	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:22:42.804510117 CEST	9387	49695	213.152.162.181	192.168.2.4
May 30, 2023 06:22:42.804651022 CEST	49695	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:22:43.246304989 CEST	9387	49695	213.152.162.181	192.168.2.4
May 30, 2023 06:22:43.246417999 CEST	49695	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:22:43.336347103 CEST	9387	49695	213.152.162.181	192.168.2.4
May 30, 2023 06:22:43.385773897 CEST	49695	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:22:43.554548979 CEST	9387	49695	213.152.162.181	192.168.2.4
May 30, 2023 06:22:43.562437057 CEST	9387	49695	213.152.162.181	192.168.2.4
May 30, 2023 06:22:43.562505960 CEST	49695	9387	192.168.2.4	213.152.162.181

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 30, 2023 06:22:43.574924946 CEST	49695	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:22:43.753716946 CEST	9387	49695	213.152.162.181	192.168.2.4
May 30, 2023 06:22:43.753774881 CEST	9387	49695	213.152.162.181	192.168.2.4
May 30, 2023 06:22:43.753797054 CEST	49695	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:22:43.753832102 CEST	49695	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:22:43.753838062 CEST	9387	49695	213.152.162.181	192.168.2.4
May 30, 2023 06:22:43.753882885 CEST	49695	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:22:43.753887892 CEST	9387	49695	213.152.162.181	192.168.2.4
May 30, 2023 06:22:43.753936052 CEST	49695	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:12.071541071 CEST	49696	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:12.264368057 CEST	9387	49696	213.152.162.181	192.168.2.4
May 30, 2023 06:23:12.264554024 CEST	49696	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:12.265300989 CEST	49696	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:12.566230059 CEST	9387	49696	213.152.162.181	192.168.2.4
May 30, 2023 06:23:12.568962097 CEST	49696	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:12.736325026 CEST	9387	49696	213.152.162.181	192.168.2.4
May 30, 2023 06:23:12.841810942 CEST	49696	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:13.042467117 CEST	9387	49696	213.152.162.181	192.168.2.4
May 30, 2023 06:23:13.051351070 CEST	49696	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:13.077162981 CEST	49696	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:41.984854937 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:42.156399965 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:42.156558037 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:42.157294989 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:42.584623098 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:42.584820032 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:42.594243050 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:42.640885115 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:42.996824980 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:42.997116089 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:43.184432983 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:43.197169065 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:43.464411020 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:43.464776039 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:43.472467899 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:43.472791910 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:43.655715942 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:43.655760050 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:43.655951977 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:43.662724018 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:43.662763119 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:43.662925005 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:43.895749092 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:43.896639109 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:43.896739006 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:43.896821976 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:43.896871090 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:43.896961927 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:43.903920889 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:43.904055119 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:43.904135942 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:43.904166937 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:43.904218912 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:43.904304028 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:44.075617075 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.075689077 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.075803995 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:44.076646090 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.076699018 CEST	9387	49697	213.152.162.181	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 30, 2023 06:23:44.076745987 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.076766968 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:44.076797962 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.076843977 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.076858997 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:44.083528042 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.083578110 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.083625078 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.083671093 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.083718061 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.083715916 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:44.083802938 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:44.084388971 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.084436893 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.084511042 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.084558964 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.084599018 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:44.084656954 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:44.315434933 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.315506935 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.315670013 CEST	49697	9387	192.168.2.4	213.152.162.181
May 30, 2023 06:23:44.316407919 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.316462040 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.316548109 CEST	9387	49697	213.152.162.181	192.168.2.4
May 30, 2023 06:23:44.316593885 CEST	9387	49697	213.152.162.181	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 30, 2023 06:22:16.854002953 CEST	59683	53	192.168.2.4	37.235.1.174
May 30, 2023 06:22:18.062854052 CEST	59683	53	192.168.2.4	37.235.1.174
May 30, 2023 06:22:19.104496002 CEST	59683	53	192.168.2.4	37.235.1.174
May 30, 2023 06:22:21.104768991 CEST	59683	53	192.168.2.4	37.235.1.174
May 30, 2023 06:22:25.133699894 CEST	59683	53	192.168.2.4	37.235.1.174
May 30, 2023 06:22:29.209393024 CEST	64167	53	192.168.2.4	37.235.1.177
May 30, 2023 06:22:30.228588104 CEST	64167	53	192.168.2.4	37.235.1.177
May 30, 2023 06:22:31.275765896 CEST	64167	53	192.168.2.4	37.235.1.177
May 30, 2023 06:22:33.297673941 CEST	64167	53	192.168.2.4	37.235.1.177
May 30, 2023 06:22:37.396856070 CEST	64167	53	192.168.2.4	37.235.1.177
May 30, 2023 06:22:41.471667051 CEST	61007	53	192.168.2.4	8.8.8.8
May 30, 2023 06:22:41.498262882 CEST	53	61007	8.8.8.8	192.168.2.4
May 30, 2023 06:22:47.655108929 CEST	60686	53	192.168.2.4	37.235.1.174
May 30, 2023 06:22:48.653067112 CEST	60686	53	192.168.2.4	37.235.1.174
May 30, 2023 06:22:49.652857065 CEST	60686	53	192.168.2.4	37.235.1.174
May 30, 2023 06:22:51.699614048 CEST	60686	53	192.168.2.4	37.235.1.174
May 30, 2023 06:22:55.731234074 CEST	60686	53	192.168.2.4	37.235.1.174
May 30, 2023 06:22:59.801834106 CEST	61124	53	192.168.2.4	37.235.1.177
May 30, 2023 06:23:00.830032110 CEST	61124	53	192.168.2.4	37.235.1.177
May 30, 2023 06:23:01.873676062 CEST	61124	53	192.168.2.4	37.235.1.177
May 30, 2023 06:23:03.963443995 CEST	61124	53	192.168.2.4	37.235.1.177
May 30, 2023 06:23:07.951122046 CEST	61124	53	192.168.2.4	37.235.1.177
May 30, 2023 06:23:12.028436899 CEST	59444	53	192.168.2.4	8.8.8.8
May 30, 2023 06:23:12.056085110 CEST	53	59444	8.8.8.8	192.168.2.4
May 30, 2023 06:23:17.136106014 CEST	55570	53	192.168.2.4	37.235.1.174
May 30, 2023 06:23:18.196037054 CEST	55570	53	192.168.2.4	37.235.1.174
May 30, 2023 06:23:19.233864069 CEST	55570	53	192.168.2.4	37.235.1.174
May 30, 2023 06:23:21.248723030 CEST	55570	53	192.168.2.4	37.235.1.174
May 30, 2023 06:23:25.280725956 CEST	55570	53	192.168.2.4	37.235.1.174
May 30, 2023 06:23:29.805553913 CEST	64906	53	192.168.2.4	37.235.1.177

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 30, 2023 06:23:30.812082052 CEST	64906	53	192.168.2.4	37.235.1.177
May 30, 2023 06:23:31.828206062 CEST	64906	53	192.168.2.4	37.235.1.177
May 30, 2023 06:23:33.875144958 CEST	64906	53	192.168.2.4	37.235.1.177
May 30, 2023 06:23:37.921946049 CEST	64906	53	192.168.2.4	37.235.1.177
May 30, 2023 06:23:41.955786943 CEST	59446	53	192.168.2.4	8.8.8.8
May 30, 2023 06:23:41.981828928 CEST	53	59446	8.8.8.8	192.168.2.4
May 30, 2023 06:23:48.423970938 CEST	50861	53	192.168.2.4	37.235.1.174
May 30, 2023 06:23:49.425367117 CEST	50861	53	192.168.2.4	37.235.1.174
May 30, 2023 06:23:50.439079046 CEST	50861	53	192.168.2.4	37.235.1.174
May 30, 2023 06:23:52.485939980 CEST	50861	53	192.168.2.4	37.235.1.174
May 30, 2023 06:23:56.486330986 CEST	50861	53	192.168.2.4	37.235.1.174
May 30, 2023 06:24:00.524131060 CEST	61088	53	192.168.2.4	37.235.1.177
May 30, 2023 06:24:01.533629894 CEST	61088	53	192.168.2.4	37.235.1.177
May 30, 2023 06:24:02.533974886 CEST	61088	53	192.168.2.4	37.235.1.177
May 30, 2023 06:24:04.790138960 CEST	61088	53	192.168.2.4	37.235.1.177
May 30, 2023 06:24:13.178560972 CEST	61088	53	192.168.2.4	37.235.1.177

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 30, 2023 06:22:16.854002953 CEST	192.168.2.4	37.235.1.174	0x5602	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:18.062854052 CEST	192.168.2.4	37.235.1.174	0x5602	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:19.104496002 CEST	192.168.2.4	37.235.1.174	0x5602	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:21.104768991 CEST	192.168.2.4	37.235.1.174	0x5602	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:25.133699894 CEST	192.168.2.4	37.235.1.174	0x5602	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:29.209393024 CEST	192.168.2.4	37.235.1.177	0xc79c	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:30.228588104 CEST	192.168.2.4	37.235.1.177	0xc79c	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:31.275765896 CEST	192.168.2.4	37.235.1.177	0xc79c	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:33.297673941 CEST	192.168.2.4	37.235.1.177	0xc79c	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:37.396856070 CEST	192.168.2.4	37.235.1.177	0xc79c	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:41.471667051 CEST	192.168.2.4	8.8.8.8	0x76ec	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:47.655108929 CEST	192.168.2.4	37.235.1.174	0xfeb	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:48.653067112 CEST	192.168.2.4	37.235.1.174	0xfeb	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:49.652857065 CEST	192.168.2.4	37.235.1.174	0xfeb	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:51.699614048 CEST	192.168.2.4	37.235.1.174	0xfeb	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:55.731234074 CEST	192.168.2.4	37.235.1.174	0xfeb	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:22:59.801834106 CEST	192.168.2.4	37.235.1.177	0xce51	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:00.830032110 CEST	192.168.2.4	37.235.1.177	0xce51	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:01.873676062 CEST	192.168.2.4	37.235.1.177	0xce51	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:03.963443995 CEST	192.168.2.4	37.235.1.177	0xce51	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:07.951122046 CEST	192.168.2.4	37.235.1.177	0xce51	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:12.028436899 CEST	192.168.2.4	8.8.8.8	0xee70	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:17.136106014 CEST	192.168.2.4	37.235.1.174	0xba1	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 30, 2023 06:23:18.196037054 CEST	192.168.2.4	37.235.1.174	0xba1	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:19.233864069 CEST	192.168.2.4	37.235.1.174	0xba1	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:21.248723030 CEST	192.168.2.4	37.235.1.174	0xba1	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:25.280725956 CEST	192.168.2.4	37.235.1.174	0xba1	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:29.805553913 CEST	192.168.2.4	37.235.1.177	0x2c1f	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:30.812082052 CEST	192.168.2.4	37.235.1.177	0x2c1f	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:31.828206062 CEST	192.168.2.4	37.235.1.177	0x2c1f	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:33.875144958 CEST	192.168.2.4	37.235.1.177	0x2c1f	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:37.921946049 CEST	192.168.2.4	37.235.1.177	0x2c1f	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:41.955786943 CEST	192.168.2.4	8.8.8.8	0x5c7d	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:48.423970938 CEST	192.168.2.4	37.235.1.174	0xe6d6	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:49.425367117 CEST	192.168.2.4	37.235.1.174	0xe6d6	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:50.439079046 CEST	192.168.2.4	37.235.1.174	0xe6d6	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:52.485939980 CEST	192.168.2.4	37.235.1.174	0xe6d6	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:56.486330986 CEST	192.168.2.4	37.235.1.174	0xe6d6	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:24:00.524131060 CEST	192.168.2.4	37.235.1.177	0x88fb	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:24:01.533629894 CEST	192.168.2.4	37.235.1.177	0x88fb	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:24:02.533974886 CEST	192.168.2.4	37.235.1.177	0x88fb	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:24:04.790138960 CEST	192.168.2.4	37.235.1.177	0x88fb	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false
May 30, 2023 06:24:13.178560972 CEST	192.168.2.4	37.235.1.177	0x88fb	Standard query (0)	atelilian99.ddns.net	A (IP address)	IN (0x0001)	false

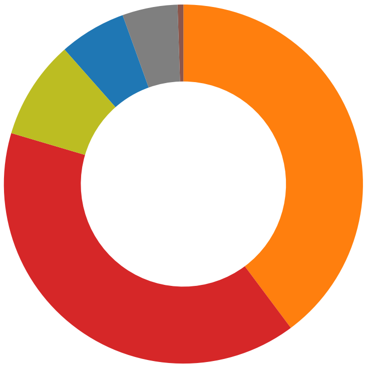
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 30, 2023 06:22:41.498262882 CEST	8.8.8.8	192.168.2.4	0x76ec	No error (0)	atelilian99.ddns.net		213.152.162.181	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:12.056085110 CEST	8.8.8.8	192.168.2.4	0xee70	No error (0)	atelilian99.ddns.net		213.152.162.181	A (IP address)	IN (0x0001)	false
May 30, 2023 06:23:41.981828928 CEST	8.8.8.8	192.168.2.4	0x5c7d	No error (0)	atelilian99.ddns.net		213.152.162.181	A (IP address)	IN (0x0001)	false

Statistics

Behavior

- CgpIx13Spu.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- unFmnPEZpvL.exe



- CgpIx13Spu.exe
- schtasks.exe
- conhost.exe
- unFmnPEZpvL.exe
- unFmnPEZpvL.exe
- dhcpmon.exe
- schtasks.exe
- conhost.exe
- dhcpmon.exe

Click to jump to process

System Behavior

Analysis Process: CgpIx13Spu.exe PID: **7060**, Parent PID: **3528**

General

Target ID:	0
Start time:	06:22:00
Start date:	30/05/2023
Path:	C:\Users\user\Desktop\CgpIx13Spu.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\CgpIx13Spu.exe
Imagebase:	0x2e0000
File size:	696320 bytes
MD5 hash:	DC586FEF0D44E3B50964F916AB75A44F
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: 00000000.00000002.564028371.0000000004274000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.564028371.0000000004274000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.564028371.0000000004274000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.564028371.0000000004274000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.564028371.0000000003731000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.564028371.0000000003731000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.564028371.0000000003731000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.564028371.0000000003731000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	72E1CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	72E1CF06	unknown
C:\Users\user\AppData\Roaming\unFmnPEZpvL.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	71C6DD66	CopyFileW
C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	71C6DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7EB8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71C67038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CgpIx13Spu.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7312C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7EB8.tmp	success or wait	1	71C66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\unFmnPEZpvL.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 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 16 fd fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 0a 00 00 08 00 00 00 00 00 00 72 fd 0a 00 00 20 00 00 00 fd 0a 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 00 0b 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.$PEL0r @ @	success or wait	3	71C6DD66	CopyFileW
C:\Users\user\AppData\Roaming\unFmnPEZpvL.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	71C6DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7EB8.tmp	0	1598	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationInfo>	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CgpIx13Spu.exe.log	0	1302	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	7312C907	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	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile

Analysis Process: powershell.exe PID: **1412**, Parent PID: **7060**

General

Target ID:	2
Start time:	06:22:05
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\CgpIx13Spu.exe
Imagebase:	0x10c0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71BC5B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71BC5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2vfoed4z.egy.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71C61E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xc2sbisk.3fp.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71C61E60	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	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	72E1CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2vfoed4z.egy.ps1	success or wait	1	71C66A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xc2sbisk.3fp.psm1	success or wait	1	71C66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71BC5B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71BC5B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71BC5B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71BC5B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71BC5B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71BC5B28	unknown
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2vfoed4z.egy.ps1	0	1	31	1	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xc2sbisk.3fp.psm1	0	1	31	1	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 1b 14 00 00 18 00 00 00 fd 0e fd 03 fd 0a fd 0a fd 0a 00 00 28 01 fd 00 0e 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00 00	@e(@	success or wait	1	730E76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	730E76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	730E76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	730E76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	730E76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 16 3b 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 fd 3c 40 01 57 03 40 01 4d 03 40 01 fd 45 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 42 4d 00 01 fd 44 00 01 6d 45 00	T@>@@V@H@X@[@NT@HT@;@S@S@hT@S@ S@S@\@T@T@@X@?X@T@S@S@T@T@xT@z T@T@=M@DM@:M@"M@ M@!M@;@;@<@<@<@W@M@E@;M@D@D@@M@<M@$M@8M@?M@BMDmE	success or wait	11	730E76FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DFCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DFCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	72E01F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22384	success or wait	1	72E0203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	71C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	71C61B4F	ReadFile

Analysis Process: conhost.exe PID: **5200**, Parent PID: **1412**

General

Target ID:	3
Start time:	06:22:05
Start date:	30/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: powershell.exe PID: **4028**, Parent PID: **7060**

General

Target ID:	4
Start time:	06:22:05
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe
Imagebase:	0x10c0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71BC5B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71BC5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_etowe3li.cjh.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71C61E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_r4xwpnyv.mvb.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71C61E60	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	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	72E1CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_etowe3li.cjh.ps1	success or wait	1	71C66A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_r4xwpnyv.mvb.psm1	success or wait	1	71C66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	122	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71BC5B28	unknown
unknown	141	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71BC5B28	unknown
unknown	162	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71BC5B28	unknown
unknown	178	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71BC5B28	unknown
unknown	186	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71BC5B28	unknown
unknown	195	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71BC5B28	unknown
unknown	203	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71BC5B28	unknown
C:\Users\user\AppData\Local\Te mp__PSscr iptPolicyTest_etowe3li.cjh.ps1	0	1	31	1	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Local\Te mp__PSscr iptPolicyTest_r4xwpnyv.mvb.psm1	0	1	31	1	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Local\Mi crosoft\Windows\PowerShell\Sta rtupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 1b 14 00 00 18 00 00 00 fd 0e fd 03 fd 0a fd 0a fd 0a 00 00 28 01 fd 00 0e 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e(@	success or wait	1	730E76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	730E76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	730E76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	730E76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	730E76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 16 3b 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 fd 3c 40 01 57 03 40 01 4d 03 40 01 fd 45 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 42 4d 00 01 fd 44 00 01 6d 45 00	T@>@@V@H@X@[@NT@HT@;@S@S@hT@S@ S@S@\@T@T@@X@?X@T@S@S@T@T@xT@z T@T@=M@DM@:M@"M@ M@!M@;@;@<@<@<@W@M@E@;M@D@D@@M@<M@$M@8M@?M@BMDmE	success or wait	11	730E76FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DFCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	72E01F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22384	success or wait	1	72E0203F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	71C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	71C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	71C61B4F	ReadFile

Analysis Process: conhost.exe PID: **3984**, Parent PID: **4028**

General

Target ID:	5
Start time:	06:22:05
Start date:	30/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: schtasks.exe PID: **2344**, Parent PID: **7060**

General

Target ID:	6
Start time:	06:22:05
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\unFmnPEZpvL" /XML "C:\Users\user\AppData\Local\Temp\tmp7EB8.tmp
Imagebase:	0x200000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7EB8.tmp	unknown	2	success or wait	1	20AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7EB8.tmp	unknown	1599	success or wait	1	20ABD9	ReadFile

Analysis Process: conhost.exe PID: **7112**, Parent PID: **2344**

General

Target ID:	7
Start time:	06:22:05
Start date:	30/05/2023

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: unFmnPEZpvL.exe PID: **7336**, Parent PID: **1088**

General

Target ID:	9
Start time:	06:22:07
Start date:	30/05/2023
Path:	C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe
Imagebase:	0x410000
File size:	696320 bytes
MD5 hash:	DC586FEF0D44E3B50964F916AB75A44F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.586418916.00000000044AC000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.586418916.00000000044AC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.586418916.00000000044AC000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000009.00000002.586418916.00000000044AC000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 65%, 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	72E1CF06	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	72E1CF06	unknown
C:\Users\user\AppData\Local\Temp\tmpB1AF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71C67038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\unFmnPEZpvL.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7312C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB1AF.tmp	success or wait	1	71C66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Te mp\tmpB1AF.tmp	0	1598	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" x mlns="http://schemas.mic rosoft .com/windows/2004/02/m it/task"> <RegistrationInfo> <Date>2014-10- 25T14:27:44.8929027</ Date> <Author>computer\user </Author> </RegistrationInfo>	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Local\Mi crosoft\CLR_v4.0_32\UsageLogs\ unFmnPEZpvL.exe.log	0	1216	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,"Win RT","N otApp",12,"System.Wind ows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c 56 1934e089",03,"System, Version=4.0.0.0, Culture=neutral, Publ icKeyToken=b77a5c5619 34e089"," C:\Windows\assembly\Na tiveImages_v4.0.3	success or wait	1	7312C907	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	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuratio n.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile

Analysis Process: CgpIx13Spu.exe PID: **7456**, Parent PID: **7060**

General

Target ID:	10
Start time:	06:22:11
Start date:	30/05/2023
Path:	C:\Users\user\Desktop\CgpIx13Spu.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\CgpIx13Spu.exe
Imagebase:	0x7a0000
File size:	696320 bytes
MD5 hash:	DC586FEF0D44E3B50964F916AB75A44F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.812707754.0000000003C2B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.814395614.00000000053A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.814395614.00000000053A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.814395614.00000000053A0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.814395614.00000000053A0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.814807006.00000000055A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.814807006.00000000055A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.814807006.00000000055A0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.814807006.00000000055A0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.814807006.00000000055A0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.804694487.0000000002BE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.804694487.0000000002BE1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	72E1CF06	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	72E1CF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71C6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	71C61E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71C6BEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.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	71C6DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	71C6DD66	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71C6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71C6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	2	71C61E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\CgpIx13Spu.exe:Zone.Identifier	success or wait	1	71BE2935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	35 03 11 72 fd 60 fd 48	5r`H	success or wait	1	71C61B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.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 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 16 fd fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 0a 00 00 08 00 00 00 00 00 00 72 fd 0a 00 00 20 00 00 00 fd 0a 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 00 0b 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.$PEL0r @ @	success or wait	3	71C6DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.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	71C6DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 0b fd 73 7e fd fd 46 04 fd fd 7d fd fd fd fd fd 00 45 fd fd fd fd fd fd 45 fd 14 fd 36 45 fd fd fd fd fd 7b 5f 05 18 7b fd 79 53 fd fd fd 37 fd fd 22 16 68 4b fd 21 03 78 fd 32 fd fd 69 e3 fd 7a 4a fd bb fd 20 fd fd fd fd 66 fd 67 3f fd 5f 0b fd fd fd 30 fd 3a 65 5b 37 77 7b 31 fd 21 fd 34 fd fd fd fd fd 26 fd	Gjh\3A5x&i+c(1PPcLTAb4ht+Z\ i@ 3{grv+VB]PW4C}uLs~F}EE6E{{yS7"hK!x2izJ f? _0:e[7w{1!4&	success or wait	3	71C61B4F	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	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	72DDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	72DDD72F	unknown
C:\Users\user\Desktop\CgpIx13Spu.exe	unknown	4096	success or wait	1	72DDD72F	unknown
C:\Users\user\Desktop\CgpIx13Spu.exe	unknown	512	success or wait	1	72DDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	72DDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	72DDD72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	71C6646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **7740**, Parent PID: **7336**

General

Target ID:	12

Start time:	06:22:20
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\unFmnPEZpvL" /XML "C:\Users\user\AppData\Local\Temp\tmpB1AF.tmp
Imagebase:	0x200000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **7748**, Parent PID: **7740**

General

Target ID:	13
Start time:	06:22:20
Start date:	30/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: unFmnPEZpvL.exe PID: **7784**, Parent PID: **7336**

General

Target ID:	14
Start time:	06:22:21
Start date:	30/05/2023
Path:	C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe
Imagebase:	0x2d0000
File size:	696320 bytes
MD5 hash:	DC586FEF0D44E3B50964F916AB75A44F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: unFmnPEZpvL.exe PID: **7792**, Parent PID: **7336**

General

Target ID:	15
Start time:	06:22:21
Start date:	30/05/2023
Path:	C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\unFmnPEZpvL.exe
Imagebase:	0x5b0000
File size:	696320 bytes

MD5 hash:	DC586FEF0D44E3B50964F916AB75A44F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.596149804.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.596149804.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.596149804.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000F.00000002.596149804.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.600559154.0000000003959000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.600559154.0000000003959000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000F.00000002.600559154.0000000003959000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.599720023.0000000002951000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.599720023.0000000002951000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000F.00000002.599720023.0000000002951000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: dhcpmon.exe PID: **7852**, Parent PID: **3528**

General

Target ID:	16
Start time:	06:22:26
Start date:	30/05/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x7d0000
File size:	696320 bytes
MD5 hash:	DC586FEF0D44E3B50964F916AB75A44F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 65%, ReversingLabs

Analysis Process: schtasks.exe PID: **7916**, Parent PID: **7852**

General

Target ID:	17
Start time:	06:22:29
Start date:	30/05/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\unFmnPEZpvL" /XML "C:\Users\user\AppData\Local\Temp\tmpDAE1.tmp
Imagebase:	0x200000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **7924**, Parent PID: **7916**

General

Target ID:	18

Start time:	06:22:29
Start date:	30/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **7980**, Parent PID: **7852**

General

Target ID:	19
Start time:	06:22:30
Start date:	30/05/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x970000
File size:	696320 bytes
MD5 hash:	DC586FEF0D44E3B50964F916AB75A44F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.621550048.0000000003D9B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.621139694.0000000002D51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.621139694.0000000002D51000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.621139694.0000000002D51000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Disassembly

No disassembly