ID: 679215
Sample Name: Model list set 20 USD4 8 HPID 90CUI 874.exe
Cookbook: default.jbs
Time: 12:15:59
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

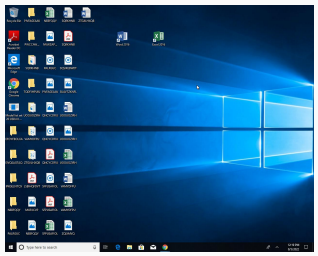
Windows Analysis Report

Model list set 20 USD4 8 HPID 90CUI 874.exe

Overview

General Information

Sample Name:	Model list set 20 USD4 8 HPID 90CUI 874.exe
Analysis ID:	679215
MD5:	583524e79bf439..
SHA1:	433e13004fc64e..
SHA256:	fded70e0d7bee0..
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

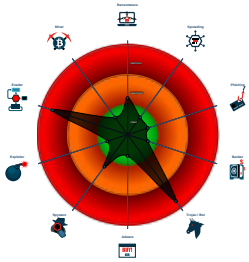
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- Machine Learning detection for drop…
- C2 URLs / IPs found in malware con…
- Adds a directory exclusion to Windo…

Classification



Process Tree

- **System is w10x64**
- Model list set 20 USD4 8 HPID 90CUI 874.exe (PID: 3248 cmdline: "C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe" MD5: 583524E79BF439FE42FC992FEA5D75F9)
  - powershell.exe (PID: 1048 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\nFxIoujoILCO.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5200 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nFxIoujoILCO" /XML "C:\Users\user\AppData\Local\Temp\tmpFC8E.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Model list set 20 USD4 8 HPID 90CUI 874.exe (PID: 3748 cmdline: C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe MD5: 583524E79BF439FE42FC992FEA5D75F9)
    - schtasks.exe (PID: 6084 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp9E33.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 2860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5940 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" / xml "C:\Users\user\AppData\Local\Temp\tmpB1FA.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6128 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Model list set 20 USD4 8 HPID 90CUI 874.exe (PID: 6140 cmdline: "C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe" 0 MD5: 583524E79BF439FE42FC992FEA5D75F9)
  - powershell.exe (PID: 340 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\nFxIoujoILCO.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1232 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 1796 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nFxIoujoILCO" /XML "C:\Users\user\AppData\Local\Temp\tmpA793.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5516 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Model list set 20 USD4 8 HPID 90CUI 874.exe (PID: 4196 cmdline: C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe MD5: 583524E79BF439FE42FC992FEA5D75F9)
- dhcpmon.exe (PID: 6016 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 583524E79BF439FE42FC992FEA5D75F9)
  - powershell.exe (PID: 3568 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\nFxIoujoILCO.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 1004 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nFxIoujoILCO" /XML "C:\Users\user\AppData\Local\Temp\tmpB53F.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5264 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 5516 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 583524E79BF439FE42FC992FEA5D75F9)
- dhcpmon.exe (PID: 3656 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 583524E79BF439FE42FC992FEA5D75F9)

- powershell.exe (PID: 3264 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\nFxIoujoILCO.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 1428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- schtasks.exe (PID: 1288 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nFxIoujoILCO" /XML "C:\Users\user\AppData\Local\Temp\tmpC3B6.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
  - conhost.exe (PID: 6128 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 5004 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 583524E79BF439FE42FC992FEA5D75F9)

cleanup

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "7492bd48-e55d-4165-b6f8-ba286e7d",
  "Group": "Default",
  "Domain1": "79.134.225.53",
  "Domain2": "79.134.225.53",
  "Port": 7171,
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "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",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.547137638.00000000064F0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
0000000A.00000002.547137638.00000000064F0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
0000000A.00000002.547137638.00000000064F0000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000A.00000002.547137638.00000000064F0000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xf778:$x2: NanoCore.ClientPlugin • 0xf7ad:$x3: NanoCore.ClientPluginHost • 0xf76c:$i2: IClientData • 0xf78e:$i3: IClientNetwork • 0xf79d:$i5: IClientDataHost • 0xf7c7:$i6: IClientLoggingHost • 0xf7da:$i7: IClientNetworkHost • 0xf7ed:$i8: IClientUIHost • 0xf7fb:$i9: IClientNameObjectCollection • 0xf817:$i10: IClientReadOnlyNameObjectCollection • 0xf56a:$s1: ClientPlugin • 0xf781:$s1: ClientPlugin • 0x147a2:$s6: get_ClientSettings

Source	Rule	Description	Author	Strings
0000000A.00000002.547137638.00000000064F0000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xf7ad:$a1: NanoCore.ClientPluginHost • 0xf778:$a2: NanoCore.ClientPlugin • 0x146f3:$b1: get_BuilderSettings • 0x14662:$b7: LogClientException • 0xf7c7:$b9: IClientLoggingHost
Click to see the 41 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.Model list set 20 USD4 8 HPID 90CUI 874.exe.64f0000.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
10.2.Model list set 20 USD4 8 HPID 90CUI 874.exe.64f0000.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
10.2.Model list set 20 USD4 8 HPID 90CUI 874.exe.64f0000.5.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
10.2.Model list set 20 USD4 8 HPID 90CUI 874.exe.64f0000.5.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xf778:$x2: NanoCore.ClientPlugin • 0xf7ad:$x3: NanoCore.ClientPluginHost • 0xf76c:$i2: IClientData • 0xf78e:$i3: IClientNetwork • 0xf79d:$i5: IClientDataHost • 0xf7c7:$i6: IClientLoggingHost • 0xf7da:$i7: IClientNetworkHost • 0xf7ed:$i8: IClientUIHost • 0xf7fb:$i9: IClientNameObjectCollection • 0xf817:$i10: IClientReadOnlyNameObjectCollection • 0xf56a:$s1: ClientPlugin • 0xf781:$s1: ClientPlugin • 0x147a2:$s6: get_ClientSettings
10.2.Model list set 20 USD4 8 HPID 90CUI 874.exe.64f0000.5.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xf7ad:$a1: NanoCore.ClientPluginHost • 0xf778:$a2: NanoCore.ClientPlugin • 0x146f3:$b1: get_BuilderSettings • 0x14662:$b7: LogClientException • 0xf7c7:$b9: IClientLoggingHost
Click to see the 81 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

C2 URLs / IPs found in malware configuration

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)

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

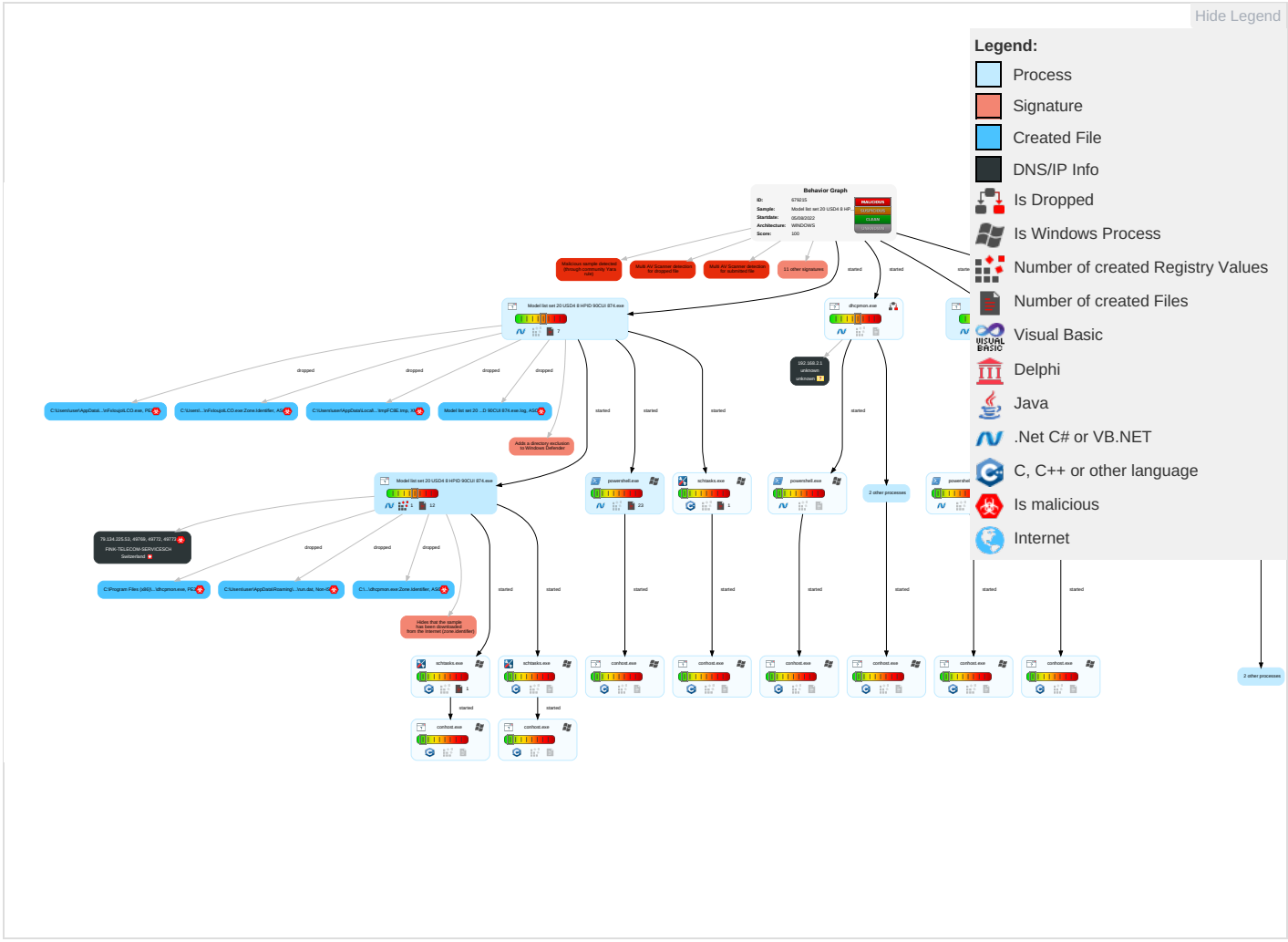
Detected Nanocore Rat

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	1 1 Input Capture	1 Query Registry	Remote Services	1 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 1 Security Software 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 Process Discovery	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	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 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 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 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	2 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 3 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

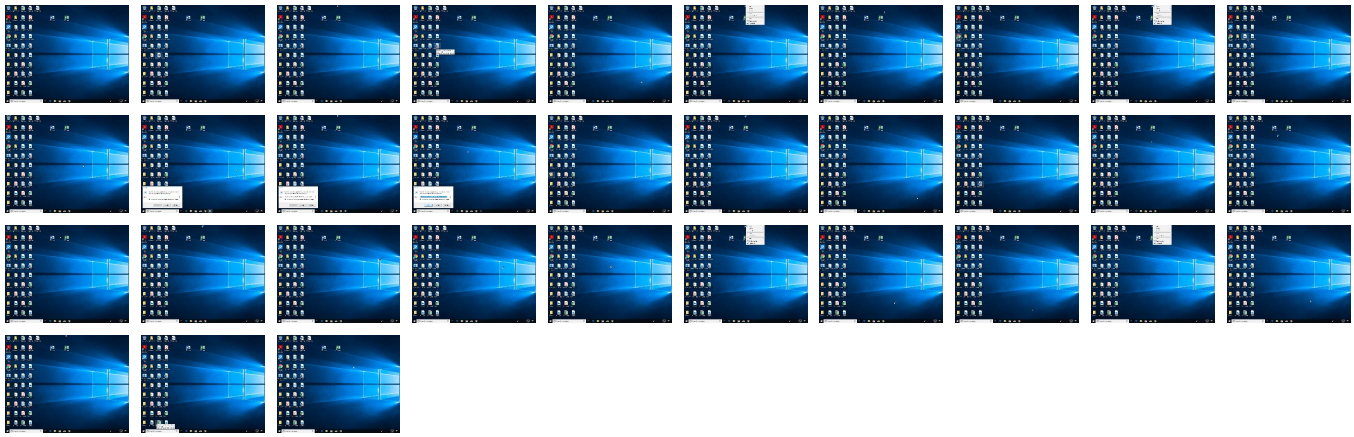
Behavior Graph



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
Model list set 20 USD4 8 HPID 90CUI 874.exe	35%	Virustotal		Browse
Model list set 20 USD4 8 HPID 90CUI 874.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\nFxIoujoILCO.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	42%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
C:\Users\user\AppData\Roaming\nFxIoujoILCO.exe	42%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.0.Model list set 20 USD4 8 HPID 90CUI 874.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.2.Model list set 20 USD4 8 HPID 90CUI 874.exe.64f0000.5.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

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	
79.134.225.53	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	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.founder.com.cn/cn	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.sandoll.co.kr	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	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
79.134.225.53	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.goodfont.co.kr	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.314747200.0000000002D44000.00000004.00000800.00020000.00000000.sdmp, Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000015.00000002.447427270.0000000003640000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 00000018.00000002.480519748.00000000003302000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 00000019.00000002.481015989.0000000002E12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	Model list set 20 USD4 8 HPID 90CUI 874.exe, 00000000.00000002.336683210.0000000006E62000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.53	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679215
Start date and time: 05/08/202212:15:59	2022-08-05 12:15:59 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Model list set 20 USD4 8 HPID 90CUI 874.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	44
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.evad.winEXE@41/28@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 80.67.82.211, 80.67.82.235
- Excluded domains from analysis (whitelisted): www.bing.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, img-prod-cms-rt-microsoft-com.akamaized.net, a1449.dscg2.akamai.net, arc.msn.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
12:17:20	API Interceptor	527x Sleep call for process: Model list set 20 USD4 8 HPID 90CUI 874.exe modified
12:17:34	API Interceptor	160x Sleep call for process: powershell.exe modified
12:17:44	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
12:17:51	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe" s>$(Arg0)
12:17:56	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
12:18:02	API Interceptor	2x 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\Model list set 20 USD4 8 HPID 90CUI 874.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	800768
Entropy (8bit):	7.534745522724267
Encrypted:	false
SSDEEP:	24576:/l4lNlPllllplUlllllllllllllUlUUPllllUlUllbUllbT9dDZH1m3q+lVKbk0Q:/l4lNlPllllplUlllllllllllllUlUUt
MD5:	583524E79BF439FE42FC992FEA5D75F9
SHA1:	433E13004FC64EF09412E0AC57CC42492EB9B327
SHA-256:	FDED70E0D7BEE0D44FDB8CD327A09F1A879D61CC35A57A4D2CBA7D7D232EED18
SHA-512:	B7B1E704C7FFD7993FC937D63D0C49BC3A359CE963DC15CFB29276B282FAD8DDD3035ACBD9EBF3211A01BEB87C1C89D717716CE8876B9E51040B0F0F1186E62
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 42%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....NL... ...`....@.. ..... ..@.....K..O....`.....K..... ....H.....text...l,... ....`.rsrc.....`.....0.....@..@.rel oc.....6.....@..B.....0L.....H.....@....O.....$...8....y.....}.....(.....(.....{....o.....*....0..w.....r...p..s.....~O....o....r$..p..B....(.... ...s.....o.....s.....o.....{.....o.....&.....,..o.....*.....Tc.....]k.....0..:.....o .....,+..{....o!...o"....o#...o$....B.....(.....*...0..n.....r...p..s.....o.....r...p..B...(%.....(&.....B...('.....s.....o(....r...p()...&...&.....,..o.....*.....KZ..

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

Process:	C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Model list set 20 USD4 8 HPID 90CUI 874.exe.log

Process:	C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1750
Entropy (8bit):	5.3375092442007315
Encrypted:	false
SSDEEP:	48:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzvFHYHKlEHUzvAHj:Pq5qXEwCYqhQnoPtIxHeqzN4qm0z4D
MD5:	92FEE17DD9A6925BA2D1E5EF2CD6E5F2
SHA1:	4614AE0DD188A0FE1983C5A8D82A69AF5BD13039
SHA-256:	67351D6FA9F9E11FD21E72581AFDC8E63A284A6080D99A6390641FC11C667235
SHA-512:	C599C633D288B845A7FAA31FC0FA86EAB8585CC2C515D68CA0DFC6AB16B27515A5D729EF535109B2CDE29FF3CF4CF725F4F920858501A2421FC7D76C804F2A7
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, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1750
Entropy (8bit):	5.3375092442007315
Encrypted:	false
SSDEEP:	48:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzvFHYHKlEHUzvAHj:Pq5qXEwCYqhQnoPtIxHeqzN4qm0z4D
MD5:	92FEE17DD9A6925BA2D1E5EF2CD6E5F2
SHA1:	4614AE0DD188A0FE1983C5A8D82A69AF5BD13039
SHA-256:	67351D6FA9F9E11FD21E72581AFDC8E63A284A6080D99A6390641FC11C667235
SHA-512:	C599C633D288B845A7FAA31FC0FA86EAB8585CC2C515D68CA0DFC6AB16B27515A5D729EF535109B2CDE29FF3CF4CF725F4F920858501A2421FC7D76C804F2A7
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\ModuleAnalysisCache

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.996142136926143
Encrypted:	false
SSDEEP:	384:SEdVoGIpN6KQkj2Zkjh4iUxZvuiOOdBCNXp5nYoJib4J:SYV3IpNBQkj2Yh4iUxZvuiOOdBCNZlYO
MD5:	B7D3A4EB1F0AED131A6E0EDF1D3C0414
SHA1:	A72E0DDE5F3083632B7242D2407658BCA3E54F29
SHA-256:	8E0EB5898DDF86FE9FE0011DD7AC6711BB0639A8707053D831FB348F9658289B
SHA-512:	F9367BBEC9A44E5C08757576C56B9C8637D8A0A9D6220DE925255888E6A0A088C653E207E211A6796F6A7F469736D538EA5B9E094944316CF4E8189DDD3EED9
Malicious:	false
Preview:	PSMODULECACHE.....Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

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):	22280
Entropy (8bit):	5.597761951675562
Encrypted:	false
SSDEEP:	384:KtCDLq0w+6j/pN3cSBKncjuItl/Op2eQ99gbZpo3xuT1ManZlbAV7eWjeoZBDl+R:w/pO4KcCltwu2t8lckCefw5BVb
MD5:	616990506605E1D3409054149242E57E
SHA1:	2B225EA09F826912ED1E2BAA67C3E7F5DEFD0138
SHA-256:	9A24046C7BAFD58124A743A112CF794E7A35818BBDBCF0974E180F753B925CE2
SHA-512:	17F2ACF0C71CA565F1DDBBDD0852B6882EC6027684EEF0078D828B8C07AF9708B72927D01CB5DE94C88D0EF1CA5335E67F02B1DAB4F5187C704E941BCAD2AF7
Malicious:	false
Preview:	@...e.....|.....x...p.f.f...q.g...Y.....@.....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_1wgjgr10.emd.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dnqcwgt3.nev.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_erbalgdo.umm.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qoruwi4o.wdn.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A

Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_sqj1ukds.4hk.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uijqcaea.sxq.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_x1m3aeoc.xr4.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_zd4jj05q.4ph.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp9E33.tmp

Process:	C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1329
Entropy (8bit):	5.126001463675773
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0YUQh8xtn:cbk4oL600QydbQxIYODOLedq38j
MD5:	1BE73B892B1B2842D41857E2DA179177
SHA1:	ABD247312BF56422F992A1ED3D27EB649AE8BAF7
SHA-256:	ECF7A4A0B238862F29F0DD441034FD183C7EA8805AF4182635A8FF250379AF8C
SHA-512:	6C090F199CAE30045A2956C4DEAEB3A5817D2D33559B6C78A6F98B05F588C111B15A1DA249860713A91D1A9E18DD823362382C3AB45F57E1E7956D8E045C711A
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 />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpA793.tmp

Process:	C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1599
Entropy (8bit):	5.138885676183854
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNta+xvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTvv
MD5:	26B224DEC942BFE0E97DF1095F3D7902
SHA1:	AB8AF393D15B18D3065B48F0675533B43FCE634B
SHA-256:	116FD77859645C3677CD27A6D3F928732CF70EB64C487D469B938AA1BD78D502
SHA-512:	0184579976F452E9145E40BC2CDDD78A8774BD0C156D7C67B8991C62E9BC653E9CD8953C69632A3E6D88D459ED3423D6626D0BD6EAA12FF7BA5D8A6BC307B5 7
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\tmpB1FA.tmp

Process:	C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733 4

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 />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpB53F.tmp

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1599
Entropy (8bit):	5.138885676183854
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNta+xvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTvv
MD5:	26B224DEC942BFE0E97DF1095F3D7902
SHA1:	AB8AF393D15B18D3065B48F0675533B43FCE634B
SHA-256:	116FD77859645C3677CD27A6D3F928732CF70EB64C487D469B938AA1BD78D502
SHA-512:	0184579976F452E9145E40BC2CDDD78A8774BD0C156D7C67B8991C62E9BC653E9CD8953C69632A3E6D88D459ED3423D6626D0BD6EAA12FF7BA5D8A6BC307B57
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\tmpC3B6.tmp

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1599
Entropy (8bit):	5.138885676183854
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNta+xvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTvv
MD5:	26B224DEC942BFE0E97DF1095F3D7902
SHA1:	AB8AF393D15B18D3065B48F0675533B43FCE634B
SHA-256:	116FD77859645C3677CD27A6D3F928732CF70EB64C487D469B938AA1BD78D502
SHA-512:	0184579976F452E9145E40BC2CDDD78A8774BD0C156D7C67B8991C62E9BC653E9CD8953C69632A3E6D88D459ED3423D6626D0BD6EAA12FF7BA5D8A6BC307B57
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\tmpFC8E.tmp

Process:	C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1599
Entropy (8bit):	5.138885676183854
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNta+xvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTvv
MD5:	26B224DEC942BFE0E97DF1095F3D7902
SHA1:	AB8AF393D15B18D3065B48F0675533B43FCE634B
SHA-256:	116FD77859645C3677CD27A6D3F928732CF70EB64C487D469B938AA1BD78D502
SHA-512:	0184579976F452E9145E40BC2CDDD78A8774BD0C156D7C67B8991C62E9BC653E9CD8953C69632A3E6D88D459ED3423D6626D0BD6EAA12FF7BA5D8A6BC307B57
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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:SFZuTl:SjuB
MD5:	4F2F32369E4B1BB01CA10D9B2EFA54F0
SHA1:	8F33008C609D157E0958B4DB30C186E2A4C540C4
SHA-256:	8807B9317E9086A4D675DD271CE2D24215C5AAC57E63C1ED1B869D3DE64E1A41
SHA-512:	7DA51636C6C108945AD8EEF04FD86B85D7C64465F815BE73217DE29E7E9C65734D479849C68D6B7AA737A6C1FD17C82A4FCDD05794ADB53366B44BA1892A882
Malicious:	**true**
Preview:	..`..v.H

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

Process:	C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	4.556806097125364
Encrypted:	false
SSDEEP:	3:oNt+WfWoasF7sAj7lnAFcxkjdA:oNwvon7hjxAKkhA
MD5:	37A2B653430529DD34BB5EDBFE18185F
SHA1:	3312F146E15933F9D0FA823957154A01F508895C
SHA-256:	2EE1F0208E5B8FE8EAE064D1789354DEBB4F49D6E0A782D2896E4A62B064B444
SHA-512:	117423BB6A57198A51BA0CCEA0C2D07FB22CE21E468399085F5E3114181FDE92701C70B89C157A0199385F9C9579A88588DE4CFF5BFCE429F9E91B7531BB94BE
Malicious:	false
Preview:	C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe

C:\Users\user\AppData\Roaming\nFxIoujoILCO.exe

Process:	C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	800768
Entropy (8bit):	7.534745522724267
Encrypted:	false
SSDEEP:	24576:/l4lNlPllllplUlllllllllllllUlUUPllllUlUllbUllbT9dDZH1m3q+lVKbk0Q:/l4lNlPllllplUlllllllllllllUlUUt
MD5:	583524E79BF439FE42FC992FEA5D75F9
SHA1:	433E13004FC64EF09412E0AC57CC42492EB9B327
SHA-256:	FDED70E0D7BEE0D44FDB8CD327A09F1A879D61CC35A57A4D2CBA7D7D232EED18
SHA-512:	B7B1E704C7FFD7993FC937D63D0C49BC3A359CE963DC15CFB29276B282FAD8DDD3035ACBD9EBF3211A01BEB87C1C89D717716CE8876B9E51040B0F0F1186E62
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 42%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....NL... ...`....@.. ..... ..@.....K..O....`.....K..... ....H.....text...l,... ....`.rsrc.....`.....0.....@..@.rel oc.....6.....@..B.....0L.....H.....@....O.....$...8....y.....}.....(.....(.....{.....o.....*....0..w.....r...p..s.....~O.....o.....r$..p..B....(.... ...s.....o.....s.....o.....{.....o.....&.....,..o.....*.....Tc.....]k.....0..:.....o .....,+..{....o!...o"....o#...o$...B.....(.....*...0..n.....r...p..s.....o.....r...p..B...(%.....(&.....B...('.....s.....o(.....r...p()...&...&.....,..o.....*.....KZ..

C:\Users\user\AppData\Roaming\nFxIoujoILCO.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.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

C:\Users\user\Documents\20220805\PowerShell_transcript.910646.7Hsei++w.20220805121823.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5797
Entropy (8bit):	5.397580080563146
Encrypted:	false
SSDEEP:	96:BZFjQNDaqDo1ZKZUjQNDaqDo1ZroawjZyjQNDaqDo1ZJ5AA9ZK:0Jrn
MD5:	49855611BDC60DB630A5ACCA2639B968
SHA1:	4AFD0B7636D2867877FEEEFB9E8F0824409469F3
SHA-256:	C731324EF480BDC4E24ADF92146427E826902FC04374BC6125CC51B771E9A04D
SHA-512:	1E8BC7A33BA29F1741960B07D6F50080AEF20A30DB9C3C0A684FCEC26CF10AFD8D9072E8B9983A7E5541CC863FEAA4AD85C02CA6755BD2FA8DADBB219F6D6EEB
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220805121831..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 910646 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\nFxIoujoILCO.exe..Process ID: 3264..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220805121831..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\nFxIoujoILCO.exe..**********..Windows PowerShell transcript start..Start time: 20220805122354..Username: computer\user..RunAs User: computer\

C:\Users\user\Documents\20220805\PowerShell_transcript.910646.EAOWkAOD.20220805121813.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5794
Entropy (8bit):	5.394083045375996
Encrypted:	false
SSDEEP:	96:BZbjQNCqDo1ZsZ/jQNCqDo1ZSoawjZMjQNCqDo1ZD5AAUZu:3
MD5:	052AD757BC0DF28EDAB92A893CD591A8
SHA1:	C6611A3B6BF3E5ACB384C317DC5BC0BFF5279BDE
SHA-256:	0D0FEE99EC57174F46A67C83DCEEF88A06EB0F1B753E078BA3308723ED6C5AF4
SHA-512:	FBB29FB72C2A238CB755A58C3007DD88D71831A2A274C23FC0C24EDB95046102210B9CD5220BDCA125B2A151650810DF9D064F4C71622A5AE9E42820B0C0CA6
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220805121815..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 910646 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\nFxIoujoILCO.exe..Process ID: 340..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220805121815..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\nFxIoujoILCO.exe..**********..Windows PowerShell transcript start..Start time: 20220805122216..Username: computer\user..RunAs User: computer\j

C:\Users\user\Documents\20220805\PowerShell_transcript.910646._+GsDfMQ.20220805121731.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5797

Entropy (8bit):	5.394741594200757
Encrypted:	false
SSDEEP:	96:BZTjQNwqDo1ZsZIjQNwqDo1ZooawjZ5jQNwqDo1Zf5AAnZw:S
MD5:	FB02EE14980A37D0CE5B0575B585742F
SHA1:	5D202EFB2D41D92AB6D80FD585268A1B74CB7D19
SHA-256:	70C0CDB525CB8B5BEB83E789D36AD2A72AA54F1E2D16EE00BA44F0528C907C06
SHA-512:	F22F3C661989FBF32AFB4410D457B8F81AAC75F14A3EC77981885CD1029057F64A274D92EE0A5616A9BDF763E93953971D5C63033DAD28A441728DE4F63D232E
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220805121734..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 910646 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\nFxIoujoILCO.exe..Process ID: 1048..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220805121734..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\nFxIoujoILCO.exe..**********..Windows PowerShell transcript start..Start time: 20220805122206..Username: computer\user..RunAs User: computer\

C:\Users\user\Documents\20220805\PowerShell_transcript.910646.dNNN85WC.20220805121818.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5797
Entropy (8bit):	5.398425495233895
Encrypted:	false
SSDEEP:	96:BZ+jQNFqDo1ZvZ4jQNFqDo1ZqoawjZdjQNFqDo1ZH5AAZZ6:N
MD5:	75326D7E4A6178B513E27818B18D1D2F
SHA1:	C8F8E0DCA2BFAC16F222DB4DE74B1E0844EE4EAB
SHA-256:	6C7EC60CC21FF9332D8E79FD09F6560D5BF4D104900E0211C4ABA0711234E5FD
SHA-512:	CFF2583B135B73FDEF11CAF16709E3C0818FF3FA76E22E0A48B2CAE4E1A5BCF34C05369F93067D9BEBCD2FF31BE8FD9E8AD77E7EB41E22E0E23ECAFF35F56F1A
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220805121821..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 910646 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\nFxIoujoILCO.exe..Process ID: 3568..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220805121821..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\nFxIoujoILCO.exe..**********..Windows PowerShell transcript start..Start time: 20220805122509..Username: computer\user..RunAs User: computer\

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.534745522724267
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Model list set 20 USD4 8 HPID 90CUI 874.exe
File size:	800768
MD5:	583524e79bf439fe42fc992fea5d75f9
SHA1:	433e13004fc64ef09412e0ac57cc42492eb9b327
SHA256:	fded70e0d7bee0d44fdb8cd327a09f1a879d61cc35a57a4d2cba7d7d232eed18
SHA512:	b7b1e704c7ffd7993fc937d63d0c49bc3a359ce963dc15cfb29276b282fad8ddd3035acbd9ebf3211a01beb87c1c89d717716ce8876b9e51040b0f0f1186e262
SSDEEP:	24576:/l4lNlPllllplUlllllllllllllUlUUPllllUlUllbUllbT9dDZH1m3q+lVKbk0Q:/l4lNlPllllplUlllllllllllllUlUUt
TLSH:	DE051254B2DB9753D5798FF6B46106102BB1A02F14ABF24E4C8A3CF768B1B134BA1B17
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....NL... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c4c4e
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:	0xA311829F [Sun Sep 10 17:49:19 2056 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]
dec eax
xor al, 46h
pop edx
push esp
inc edi
inc ebx
pop eax
cmp byte ptr [edi], dh
pop eax
xor al, 38h
inc edx
inc esi
aaa
xor al, 47h
inc edx
xor eax, 00003838h
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
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	0xc4bfc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc6000	0x5dc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xc4be0	0x1c	.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	0xc2c6c	0xc2e00	False	0.8279207925753689	data	7.538746478033163	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xc6000	0x5dc	0x600	False	0.427734375	data	4.148985619744162	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc8000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc6090	0x34c	data		
RT_MANIFEST	0xc63ec	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

TCP Packets

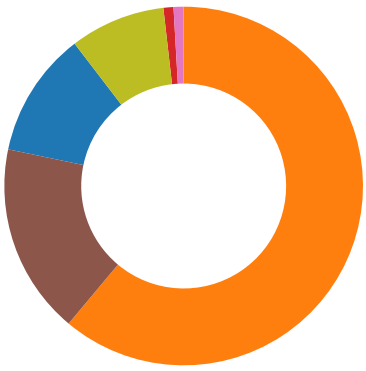
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 12:17:58.435035944 CEST	49769	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:17:58.471963882 CEST	7171	49769	79.134.225.53	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 12:17:58.996619940 CEST	49769	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:17:59.033456087 CEST	7171	49769	79.134.225.53	192.168.2.4
Aug 5, 2022 12:17:59.684570074 CEST	49769	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:17:59.721365929 CEST	7171	49769	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:03.887938023 CEST	49772	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:03.924483061 CEST	7171	49772	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:04.497108936 CEST	49772	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:04.543479919 CEST	7171	49772	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:05.184741020 CEST	49772	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:05.221554995 CEST	7171	49772	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:09.334598064 CEST	49773	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:09.384211063 CEST	7171	49773	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:09.903786898 CEST	49773	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:09.940494061 CEST	7171	49773	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:10.513238907 CEST	49773	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:10.549829960 CEST	7171	49773	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:14.918122053 CEST	49774	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:14.954912901 CEST	7171	49774	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:15.498037100 CEST	49774	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:15.535012007 CEST	7171	49774	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:16.100219965 CEST	49774	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:16.136995077 CEST	7171	49774	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:20.183224916 CEST	49775	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:20.220037937 CEST	7171	49775	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:20.810957909 CEST	49775	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:20.847714901 CEST	7171	49775	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:21.514178038 CEST	49775	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:21.551007986 CEST	7171	49775	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:27.214869976 CEST	49776	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:27.253223896 CEST	7171	49776	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:27.796008110 CEST	49776	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:27.832850933 CEST	7171	49776	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:28.499233961 CEST	49776	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:28.537417889 CEST	7171	49776	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:34.008492947 CEST	49778	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:34.045329094 CEST	7171	49778	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:34.687428951 CEST	49778	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:34.724334002 CEST	7171	49778	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:35.296586037 CEST	49778	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:35.333365917 CEST	7171	49778	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:39.401328087 CEST	49779	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:39.438174963 CEST	7171	49779	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:40.015775919 CEST	49779	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:40.052634954 CEST	7171	49779	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:40.609608889 CEST	49779	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:40.646414995 CEST	7171	49779	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:44.982207060 CEST	49780	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:45.019489050 CEST	7171	49780	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:45.703802109 CEST	49780	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:45.740581036 CEST	7171	49780	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:46.313209057 CEST	49780	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:46.350296021 CEST	7171	49780	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:50.724728107 CEST	49781	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:50.761440992 CEST	7171	49781	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:51.297944069 CEST	49781	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:51.334587097 CEST	7171	49781	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:52.001188993 CEST	49781	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:52.038055897 CEST	7171	49781	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:56.089679003 CEST	49782	7171	192.168.2.4	79.134.225.53

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 12:18:56.126812935 CEST	7171	49782	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:56.704679012 CEST	49782	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:56.741524935 CEST	7171	49782	79.134.225.53	192.168.2.4
Aug 5, 2022 12:18:57.314117908 CEST	49782	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:18:57.350953102 CEST	7171	49782	79.134.225.53	192.168.2.4
Aug 5, 2022 12:19:01.366247892 CEST	49784	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:19:01.403136015 CEST	7171	49784	79.134.225.53	192.168.2.4
Aug 5, 2022 12:19:01.908222914 CEST	49784	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:19:01.945108891 CEST	7171	49784	79.134.225.53	192.168.2.4
Aug 5, 2022 12:19:02.517750978 CEST	49784	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:19:02.554533005 CEST	7171	49784	79.134.225.53	192.168.2.4
Aug 5, 2022 12:19:07.400191069 CEST	49786	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:19:07.436901093 CEST	7171	49786	79.134.225.53	192.168.2.4
Aug 5, 2022 12:19:08.018132925 CEST	49786	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:19:08.054855108 CEST	7171	49786	79.134.225.53	192.168.2.4
Aug 5, 2022 12:19:08.707675934 CEST	49786	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:19:08.744517088 CEST	7171	49786	79.134.225.53	192.168.2.4
Aug 5, 2022 12:19:13.590540886 CEST	49787	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:19:13.628022909 CEST	7171	49787	79.134.225.53	192.168.2.4
Aug 5, 2022 12:19:14.190599918 CEST	49787	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:19:14.227343082 CEST	7171	49787	79.134.225.53	192.168.2.4
Aug 5, 2022 12:19:14.799962997 CEST	49787	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:19:14.837196112 CEST	7171	49787	79.134.225.53	192.168.2.4
Aug 5, 2022 12:19:18.850112915 CEST	49789	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:19:18.886887074 CEST	7171	49789	79.134.225.53	192.168.2.4
Aug 5, 2022 12:19:19.409729958 CEST	49789	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:19:19.446454048 CEST	7171	49789	79.134.225.53	192.168.2.4
Aug 5, 2022 12:19:20.005738974 CEST	49789	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:19:36.045500040 CEST	49796	7171	192.168.2.4	79.134.225.53
Aug 5, 2022 12:19:36.082318068 CEST	7171	49796	79.134.225.53	192.168.2.4

Statistics

Behavior



- Model list set 20 USD4 8 HPID 90C…
- powershell.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- Model list set 20 USD4 8 HPID 90C…
- schtasks.exe
- conhost.exe
- Model list set 20 USD4 8 HPID 90C…
- schtasks.exe
- conhost.exe
- dhcpmon.exe
- dhcpmon.exe
- powershell.exe
- conhost.exe
- schtasks.exe
- powershell.exe
- conhost.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- powershell.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- Model list set 20 USD4 8 HPID 90C…
- dhcpmon.exe
- dhcpmon.exe

Click to jump to process

System Behavior

Analysis Process: Model list set 20 USD4 8 HPID 90CUI 874.exe PID: **3248**, Parent PID: **6116**

General

Target ID:	0
Start time:	12:17:10
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe"
Imagebase:	0x920000
File size:	800768 bytes
MD5 hash:	583524E79BF439FE42FC992FEA5D75F9
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: 00000000.00000002.333263441.00000000048A1000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.333263441.00000000048A1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.333263441.00000000048A1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.333263441.00000000048A1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.314747200.0000000002D44000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CD1CF06	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	6CD1CF06	unknown
C:\Users\user\AppData\Roaming\nFxIoujoILCO.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	6BB6DD66	CopyFileW
C:\Users\user\AppData\Roaming\nFxIoujoILCO.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6BB6DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpFC8E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BB67038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Model list set 20 USD4 8 HPID 90CUI 874.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D02C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpFC8E.tmp	success or wait	1	6BB66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\nFxIoujoILCO.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd 11 fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 2e 0c 00 00 08 00 00 00 00 00 00 4e 4c 0c 00 00 20 00 00 00 60 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0c 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.$PEL0.NL `@ @	success or wait	4	6BB6DD66	CopyFileW
C:\Users\user\AppData\Roaming\nFxIoujoILCO.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	6BB6DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpFC8E.tmp	0	1599	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	6BB61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Model list set 20 USD4 8 HPID 90CUI874.exe.log	0	1750	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	6D02C907	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	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6CC503DE	ReadFile

Analysis Process: powershell.exe PID: **1048**, Parent PID: **3248**

General

Target ID:	4
Start time:	12:17:26
Start date:	05/08/2022
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\nFxIoujoILCO.exe
Imagebase:	0xb60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10

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

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CD1CF06	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	6CD1CF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6BAC5B28	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	6BAC5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qoruwi4o.wdn.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BB61E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dnqcwgt3.nev.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BB61E60	CreateFileW
C:\Users\user\Documents\20220805	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BB6BEFF	CreateDirectoryW
C:\Users\user\Documents\20220805\PowerShell_transcript.910646._+GsDfMQ.20220805121731.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BB61E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qoruwi4o.wdn.ps1	success or wait	1	6BB66A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dnqcwgt3.nev.psm1	success or wait	1	6BB66A95	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	6BAC5B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BAC5B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BAC5B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BAC5B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BAC5B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BAC5B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BAC5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qoruwi4o.wdn.ps1	0	1	31	1	success or wait	1	6BB61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_dnqcwgt3.nev.psm1	0	1	31	1	success or wait	1	6BB61B4F	WriteFile
C:\Users\user\Documents\20220805\PowerShell_transcript.910646._+GsDfMQ.20220805121731.txt	0	3	ff		success or wait	1	6BB61B4F	WriteFile
C:\Users\user\Documents\20220805\PowerShell_transcript.910646._+GsDfMQ.20220805121731.txt	3	679	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 38 30 35 31 32 31 37 33 34 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 39 31 30 36 34 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********Windows PowerShell transcript startStart time: 20220805121734Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 910646 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	44	6BB61B4F	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 7c 14 00 00 17 00 00 00 78 0c 07 05 70 07 66 07 66 07 00 00 71 01 67 00 17 00 59 0c 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e|xpffqgY@	success or wait	1	6CFE76FC	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	6CFE76FC	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	6CFE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6CFE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6CFE76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 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 01 45 4d 00 01 fd 71 00 01 fd 71 00 01 fd 53 00 01 fd 25 00 01 fd 6e 00 01 34 26 00 01 35 26 00 01 37 26 00	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@8M@?M@BMDmEEMqqS%n4&5&7&	success or wait	11	6CFE76FC	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	6CCF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CC503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CCFCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CCFCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CC503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CC503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CCF5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6CD01F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22404	success or wait	1	6CD0203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CC503DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6BB61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CC503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CCF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CCF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6BB61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6BB61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6BB61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6BB61B4F	ReadFile

Analysis Process: conhost.exe PID: **680**, Parent PID: **1048**

General

Target ID:	6
Start time:	12:17:27
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: **5200**, Parent PID: **3248**

General

Target ID:	7
Start time:	12:17:30
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nFxIoujoILCO" /XML "C:\Users\user\AppData\Local\Temp\tmpFC8E.tmp
Imagebase:	0x1290000
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\tmpFC8E.tmp	unknown	2	success or wait	1	129AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFC8E.tmp	unknown	1600	success or wait	1	129ABD9	ReadFile

Analysis Process: conhost.exe PID: **5548**, Parent PID: **5200**

General

Target ID:	8
Start time:	12:17:31
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: Model list set 20 USD4 8 HPID 90CUI 874.exe PID: **3748**, Parent PID: **3248**

General

Target ID:	10
Start time:	12:17:35
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe
Imagebase:	0x9b0000
File size:	800768 bytes
MD5 hash:	583524E79BF439FE42FC992FEA5D75F9
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: 0000000A.00000002.547137638.00000000064F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.547137638.00000000064F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.547137638.00000000064F0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.547137638.00000000064F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.547137638.00000000064F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.546838493.0000000005810000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.546838493.0000000005810000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.546838493.0000000005810000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.546838493.0000000005810000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.528845539.0000000002E31000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.307224482.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.307224482.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.307224482.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000000.307224482.0000000000402000.00000040.00000400.00020000.00000000.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	6CD1CF06	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	6CD1CF06	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	6BB6BEFF	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	6BB61E60	CreateFileW
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	6BB6BEFF	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	6BB6DD66	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	6BB6DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp9E33.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BB67038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BB61E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpB1FA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BB67038	GetTempFileNameW
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	6BB6BEFF	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	6BB6BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9E33.tmp	success or wait	1	6BB66A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpB1FA.tmp	success or wait	1	6BB66A95	DeleteFileW
C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe:Zone.Identifier	success or wait	1	6BAE2935	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	fd fd 60 fd fd 76 fd 48	`vH	success or wait	1	6BB61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Mo nitor\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 fd 11 fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 2e 0c 00 00 08 00 00 00 00 00 00 4e 4c 0c 00 00 20 00 00 00 60 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0c 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.$PEL0.NL `@ @	success or wait	4	6BB6DD66	CopyFileW
C:\Program Files (x86)\DHCP Mo nitor\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	6BB6DD66	CopyFileW
C:\Users\user\AppData\Local\Te mp\tmp9E33.tmp	0	1329	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 0d 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 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?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 /> <Triggers /> <Principals> <Principal id="Author"> <Logon Type>InteractiveToken</ LogonType>	success or wait	1	6BB61B4F	WriteFile
C:\Users\user\AppData\Roaming\ D06ED635-68F6-4E9A-955C-4899F5 F57B9A\task.dat	0	66	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 4d 6f 64 65 6c 20 6c 69 73 74 20 73 65 74 20 32 30 20 55 53 44 34 20 38 20 48 50 49 44 20 39 30 43 55 49 20 38 37 34 2e 65 78 65	C:\Users\user\Desktop\M odel list set 20 USD4 8 HPID 90CUI 874.exe	success or wait	1	6BB61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB1FA.tmp	0	1310	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 0d 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 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	6BB61B4F	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	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6CCDD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6CCDD72F	unknown
C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe	unknown	4096	success or wait	1	6CCDD72F	unknown
C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe	unknown	512	success or wait	1	6CCDD72F	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	6BB6646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **6084**, Parent PID: **3748**

General	
Target ID:	19
Start time:	12:17:49
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp9E33.tmp
Imagebase:	0x1290000
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\tmp9E33.tmp	unknown	2	success or wait	1	129AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9E33.tmp	unknown	1330	success or wait	1	129ABD9	ReadFile

Analysis Process: conhost.exe PID: **2860**, Parent PID: **6084**

General	
Target ID:	20
Start time:	12:17:51
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
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: Model list set 20 USD4 8 HPID 90CUI 874.exe PID: **6140**, Parent PID: **960**

General	
Target ID:	21
Start time:	12:17:51
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe" 0
Imagebase:	0xea0000
File size:	800768 bytes
MD5 hash:	583524E79BF439FE42FC992FEA5D75F9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

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	6CD1CF06	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	6CD1CF06	unknown
C:\Users\user\AppData\Local\Temp\tmpA793.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BB67038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA793.tmp	success or wait	1	6BB66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA793.tmp	0	1599	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	6BB61B4F	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	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CCF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CC503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CCFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CC503DE	ReadFile

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	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CCF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BB61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BB61B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6CC503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6CC503DE	ReadFile

Analysis Process: schtasks.exe PID: **5940**, Parent PID: **3748**

General

Target ID:	22
Start time:	12:17:52
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpB1FA.tmp
Imagebase:	0x1290000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **6128**, Parent PID: **5940**

General

Target ID:	23
Start time:	12:17:54
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: **6016**, Parent PID: **3616**

General

Target ID:	24
Start time:	12:17:54
Start date:	05/08/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xc30000
File size:	800768 bytes
MD5 hash:	583524E79BF439FE42FC992FEA5D75F9

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000018.00000002.480519748.0000000003302000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 42%, ReversingLabs

Analysis Process: dhcpmon.exe PID: **3656**, Parent PID: **960**

General

Target ID:	25
Start time:	12:17:56
Start date:	05/08/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x6c0000
File size:	800768 bytes
MD5 hash:	583524E79BF439FE42FC992FEA5D75F9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: **340**, Parent PID: **6140**

General

Target ID:	26
Start time:	12:18:11
Start date:	05/08/2022
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\nFxIoujoILCO.exe
Imagebase:	0xb60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **1232**, Parent PID: **340**

General

Target ID:	27
Start time:	12:18:11
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7338d0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **1796**, Parent PID: **6140**

General	
Target ID:	28
Start time:	12:18:11
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nFxIoujoILCO" /XML "C:\Users\user\AppData\Local\Temp\tmpA793.tmp
Imagebase:	0x1290000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **3568**, Parent PID: **6016**

General	
Target ID:	29
Start time:	12:18:13
Start date:	05/08/2022
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\nFxIoujoILCO.exe
Imagebase:	0xb60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **5516**, Parent PID: **1796**

General	
Target ID:	30
Start time:	12:18:13
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5772**, Parent PID: **3568**

General	
Target ID:	31
Start time:	12:18:15
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **1004**, Parent PID: **6016**

General

Target ID:	32
Start time:	12:18:15
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nFxIoujoILCO" /XML "C:\Users\user\AppData\Local\Temp\tmpB53F.tmp
Imagebase:	0x1290000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5264**, Parent PID: **1004**

General

Target ID:	33
Start time:	12:18:16
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **3264**, Parent PID: **3656**

General

Target ID:	34
Start time:	12:18:18
Start date:	05/08/2022
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\nFxIoujoILCO.exe
Imagebase:	0xb60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **1428**, Parent PID: **3264**

General	
Target ID:	35
Start time:	12:18:18
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **1288**, Parent PID: **3656**

General	
Target ID:	36
Start time:	12:18:19
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nFxIoujoILCO" /XML "C:\Users\user\AppData\Local\Temp\tmpC3B6.tmp
Imagebase:	0x1290000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6128**, Parent PID: **1288**

General	
Target ID:	37
Start time:	12:18:21
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Model list set 20 USD4 8 HPID 90CUI 874.exe PID: **4196**, Parent PID: **6140**

General	
Target ID:	38
Start time:	12:18:22
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Model list set 20 USD4 8 HPID 90CUI 874.exe
Imagebase:	0xbf0000
File size:	800768 bytes
MD5 hash:	583524E79BF439FE42FC992FEA5D75F9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000026.00000002.512930532.0000000004049000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000026.00000002.512930532.0000000004049000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000026.00000002.512930532.0000000004049000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000026.00000002.511195057.0000000003041000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000026.00000002.511195057.0000000003041000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000026.00000002.511195057.0000000003041000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: dhcpmon.exe PID: **5516**, Parent PID: **6016**

General

Target ID:	39
Start time:	12:18:31
Start date:	05/08/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x5a0000
File size:	800768 bytes
MD5 hash:	583524E79BF439FE42FC992FEA5D75F9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000027.00000002.512811758.0000000002A91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000027.00000002.512811758.0000000002A91000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000027.00000002.512811758.0000000002A91000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: dhcpmon.exe PID: **5004**, Parent PID: **3656**

General

Target ID:	40
Start time:	12:18:35
Start date:	05/08/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xb20000
File size:	800768 bytes
MD5 hash:	583524E79BF439FE42FC992FEA5D75F9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

No disassembly