ID: 624172
Sample Name:
8v2E2Qu0iMFG7kx.exe
Cookbook: default.jbs
Time: 09:53:51
Date: 11/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

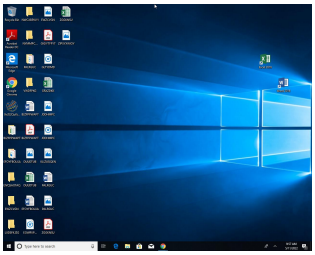
Windows Analysis Report

8v2E2Qu0iMFG7kx.exe

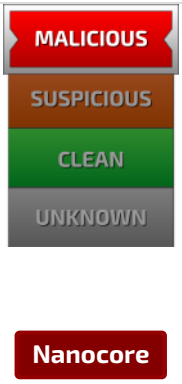
Overview

General Information

Sample Name:	8v2E2Qu0iMFG7kx.exe
Analysis ID:	624172
MD5:	a2bb923c86585a..
SHA1:	b6404adbe75431..
SHA256:	22ace1da7a25d7..
Infos:	



Detection



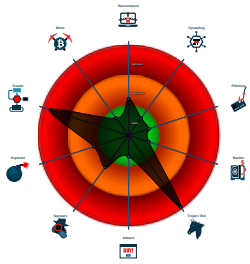
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Yara detected Nanocore RAT
- Connects to many ports of the same…
- Protects its processes via BreakOn…
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- 8v2E2Qu0iMFG7kx.exe (PID: 7112 cmdline: "C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe" MD5: A2BB923C86585AAA72A8858FB84CBC22)
  - powershell.exe (PID: 4356 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\DizKUzcAmYAC.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6468 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4384 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\DizKUzcAmYAC" /XML "C:\Users\user\AppData\Local\Temp\tmpD11B.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5220 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 8v2E2Qu0iMFG7kx.exe (PID: 3016 cmdline: C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe MD5: A2BB923C86585AAA72A8858FB84CBC22)
    - schtasks.exe (PID: 5132 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpF941.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4488 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6388 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp23B.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6172 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- 8v2E2Qu0iMFG7kx.exe (PID: 6564 cmdline: C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe 0 MD5: A2BB923C86585AAA72A8858FB84CBC22)
  - powershell.exe (PID: 4456 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\DizKUzcAmYAC.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3512 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 2984 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\DizKUzcAmYAC" /XML "C:\Users\user\AppData\Local\Temp\tmp2F0A.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 8v2E2Qu0iMFG7kx.exe (PID: 4508 cmdline: C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe MD5: A2BB923C86585AAA72A8858FB84CBC22)
  - 8v2E2Qu0iMFG7kx.exe (PID: 6084 cmdline: C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe MD5: A2BB923C86585AAA72A8858FB84CBC22)
- dhcpmon.exe (PID: 6708 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: A2BB923C86585AAA72A8858FB84CBC22)
  - powershell.exe (PID: 4004 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\DizKUzcAmYAC.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4396 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4448 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\DizKUzcAmYAC" /XML "C:\Users\user\AppData\Local\Temp\tmp3D43.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4536 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 4384 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: A2BB923C86585AAA72A8858FB84CBC22)
- dhcpmon.exe (PID: 5288 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: A2BB923C86585AAA72A8858FB84CBC22)
  - powershell.exe (PID: 5280 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\DizKUzcAmYAC.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6020 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6440 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\DizKUzcAmYAC" /XML "C:\Users\user\AppData\Local\Temp\tmp6482.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)

- conhost.exe (PID: 3240 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 7140 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: A2BB923C86585AAA72A8858FB84CBC22)
- dhcpmon.exe (PID: 6816 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: A2BB923C86585AAA72A8858FB84CBC22)

cleanup

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "3f629223-43f7-4f4e-b56f-3f91ee5e",
  "Group": "0SPEED",
  "Domain1": "lowspeed121.ddns.net",
  "Domain2": "185.19.85.175",
  "Port": 50421,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Enable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8009,
  "BufferSize": "02000100",
  "MaxPacketSize": "",
  "GCThreshold": "",
  "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
00000008.00000000.486953208.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000008.00000000.486953208.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000000.486953208.0000000000402000.00000040.00000400.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000008.00000002.715262668.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000008.00000002.715262668.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 124 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
41.0.dhcpmon.exe.400000.10.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
41.0.dhcpmon.exe.400000.10.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
41.0.dhcpmon.exe.400000.10.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
41.0.dhcpmon.exe.400000.10.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xfef5:$x1: NanoCore Client • 0xff05:$x1: NanoCore Client • 0x1014d:$x2: NanoCore.ClientPlugin • 0x1018d:$x3: NanoCore.ClientPluginHost • 0x10142:$i1: IClientApp • 0x10163:$i2: IClientData • 0x1016f:$i3: IClientNetwork • 0x1017e:$i4: IClientAppHost • 0x101a7:$i5: IClientDataHost • 0x101b7:$i6: IClientLoggingHost • 0x101ca:$i7: IClientNetworkHost • 0x101dd:$i8: IClientUIHost • 0x101eb:$i9: IClientNameObjectCollection • 0x10207:$i10: IClientReadOnlyNameObjectCollection • 0xff54:$s1: ClientPlugin • 0x10156:$s1: ClientPlugin • 0x1064a:$s2: EndPoint • 0x10653:$s3: IPAddress • 0x1065d:$s4: IPEndPoint • 0x12093:$s6: get_ClientSettings • 0x12637:$s7: get_Connected

Source	Rule	Description	Author	Strings
41.0.dhcpmon.exe.400000.10.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
Click to see the 357 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

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Networking

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

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud

Yara detected Nanocore RAT

Operating System Destruction

Protects its processes via BreakOnTermination flag

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

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

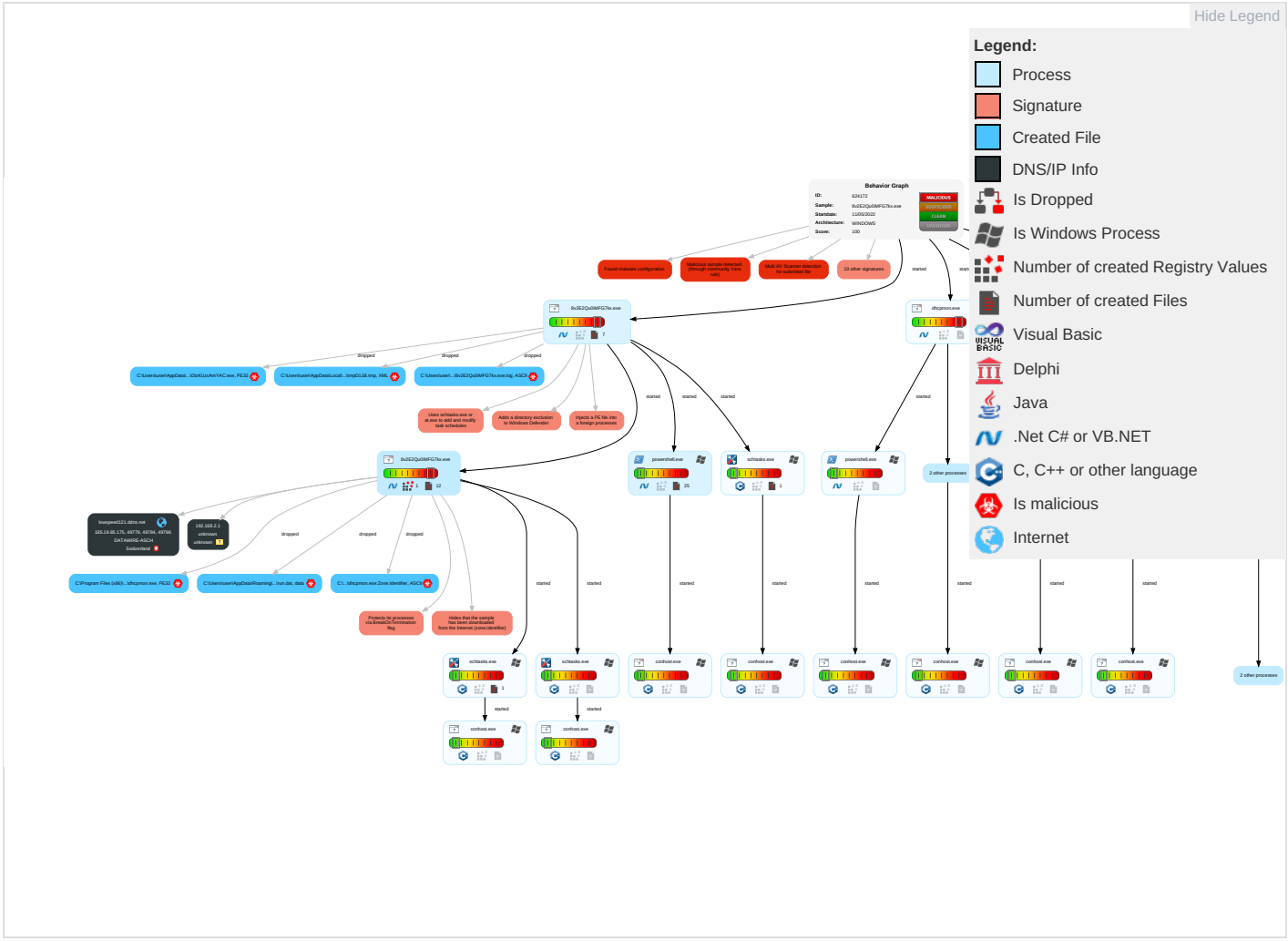
Yara detected Nanocore RAT

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 1 2 Process Injection	2 Masquerading	1 1 Input Capture	1 1 Security Software Discovery	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Obfuscated Files or Information	DCSync	1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 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

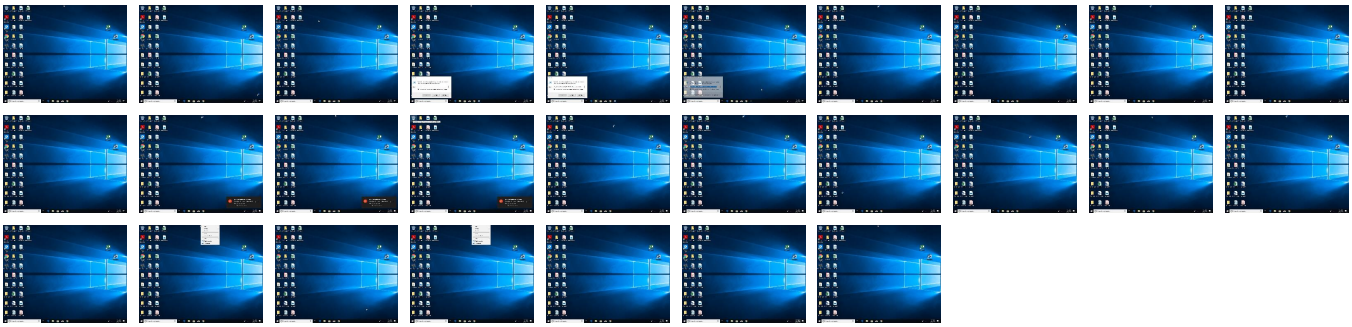
Behavior Graph



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
8v2E2Qu0iMFG7kx.exe	16%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
30.0.dhcpmon.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
41.0.dhcpmon.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
30.0.dhcpmon.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
41.0.dhcpmon.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
41.0.dhcpmon.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
41.0.dhcpmon.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
30.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.8v2E2Qu0iMFG7kx.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.8v2E2Qu0iMFG7kx.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
30.0.dhcpmon.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.8v2E2Qu0iMFG7kx.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
41.0.dhcpmon.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
32.0.8v2E2Qu0iMFG7kx.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
30.0.dhcpmon.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
32.0.8v2E2Qu0iMFG7kx.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.2.8v2E2Qu0iMFG7kx.exe.6560000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File
32.2.8v2E2Qu0iMFG7kx.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
32.0.8v2E2Qu0iMFG7kx.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
30.0.dhcpmon.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
32.0.8v2E2Qu0iMFG7kx.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
41.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
32.0.8v2E2Qu0iMFG7kx.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.8v2E2Qu0iMFG7kx.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.2.8v2E2Qu0iMFG7kx.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.8v2E2Qu0iMFG7kx.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
185.19.85.175	4%	Virustotal		Browse
185.19.85.175	0%	Avira URL Cloud	safe	
lowspeed121.ddns.net	2%	Virustotal		Browse
lowspeed121.ddns.net	0%	Avira URL Cloud	safe	
http://go.microsoft.cL/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.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://en.w-	0%	Avira URL Cloud	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	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
lowspeed121.ddns.net	185.19.85.175	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
185.19.85.175	true	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
lowspeed121.ddns.net	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://go.microsoft.cL/	dhcpmon.exe, 00000029.00000002.614762503.00000000016B2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://en.w-	8v2E2Qu0iMFG7kx.exe, 00000000.00000003.448633438.00000000012CD000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.489972165.0000000002C21000.00000004.00000800.00020000.00000000.sdmp, 8v2E2Qu0iMFG7kx.exe, 00000010.00000002.582094777.0000000002651000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 00000012.00000002.575971279.0000000002D11000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 00000014.00000002.596685149.0000000003221000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	8v2E2Qu0iMFG7kx.exe, 00000000.00000002.492844756.0000000006D32000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.19.85.175	lowspeed121.ddns.net	Switzerland		48971	DATAWIRE-ASCH	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	624172
Start date and time: 11/05/202209:53:51	2022-05-11 09:53:51 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8v2E2Qu0iMFG7kx.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:	49
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@46/27@9/2

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1.4% (good quality ratio 1.1%) • Quality average: 62.2% • Quality standard deviation: 39.3%
HCA Information:	• Successful, ratio: 98% • 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): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- 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
09:55:23	API Interceptor	787x Sleep call for process: 8v2E2Qu0iMFG7kx.exe modified
09:55:29	API Interceptor	135x Sleep call for process: powershell.exe modified
09:55:39	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe" s>$(Arg0)
09:55:39	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
09:55:42	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
09:55:48	API Interceptor	4x 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\8v2E2Qu0iMFG7kx.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	721408
Entropy (8bit):	7.8544731914193955
Encrypted:	false
SSDEEP:	12288:W0jBpXpjRAatpjiaPJxDWU/Lh7NUfMbMFEXgqA8LMPYdwo+/jJHYtop:XjBtj2aPJ1l/hN5bVwbqMQdh+/1Yto
MD5:	A2BB923C86585AAA72A8858FB84CBC22
SHA1:	B6404ADBE754315915EF021CA73309CBB4BA9EA7
SHA-256:	22ACE1DA7A25D7597434CC2EC2568A5F3E4C6CFD018FBA8251E7273340BE3DE2
SHA-512:	A194B247403D4F854698D89A3A13F43D77A15744B407C3F53C66F12CF3E82553077C51930A80D28FA5E8A5EFEB02CC4DD8920A304696049F24BB59AD8F57969D
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....\{b.....0.....Z..... .....@.. .....`..... ..@.....K.....W.....@.....e..... ..... ..H.....text..... ..... ..`.rsrc....W.....X.....@..@.rel oc.....@.....@..B.....H.....@.....b(....8.....(....8.....*....(....8.....(....8.....(....8.....*.^(.....(.....(.....*..{....*6..} ....8....*...0.....(.....8.....*.....(.....*.0..%.....8....8....8.....(....(...+..8.....*.....{....*"..}....*....0..._.....8.....*8....8.....r...p.(.....(....r...p.(.....:.....8.....o....(.....8.....0.. .....(.....8.....*..{....*"..}....*...&~.....*...~..

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

Process:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8v2E2Qu0iMFG7kx.exe.log

Process:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1750
Entropy (8bit):	5.3375092442007315
Encrypted:	false
SSDEEP:	48:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzvFHYHKlEHUzvAHj:Pq5qXEwCYqhQnoPtlxHeqzN4qm0z4D
MD5:	92FEE17DD9A6925BA2D1E5EF2CD6E5F2
SHA1:	4614AE0DD188A0FE1983C5A8D82A69AF5BD13039
SHA-256:	67351D6FA9F9E11FD21E72581AFDC8E63A284A6080D99A6390641FC11C667235
SHA-512:	C599C633D288B845A7FAA31FC0FA86EAB8585CC2C515D68CA0DFC6AB16B27515A5D729EF535109B2CDE29FF3CF4CF725F4F920858501A2421FC7D76C804F2A7
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\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
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22188
Entropy (8bit):	5.46216475932555
Encrypted:	false
SSDEEP:	384:5tMjDLpnnay0915SYsscFQCu8kMh1dInAM0+6fmAV7gHoDy3ZQvnI+++Y:AVnn/Y/psscCCtho7tepr8+Y
MD5:	B418021866CFD203750C54B46CC6122E
SHA1:	F13F0E465142F4F204C53C89AFE2F84E386B2023
SHA-256:	A9A9B69B202FC6733C5925B90EAC437E52064439D25DFA08DC58264D3E781829
SHA-512:	96317DEFCA827804423D90D0F66500035D3DAF27A21D1F6FEAF97C9A6FD07E9FC9D64C595734831E2159A68D380279206141A2EC96F5AEE0F4B4C465EC572A1
Malicious:	false
Reputation:	unknown
Preview:	@...e.....d.....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..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.4.....Zg5..:O..g..q.....System.Xml..@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....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_ccwhzi4g.sgh.ps1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_e2th3aur.tfw.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_evlpmri2.rn3.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fbqld1ow.bvq.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kifnm0ox.0v5.psm1

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

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_totha2qh.zjo.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xn2puhu2.a1t.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xuc1t3qo.n3v.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp23B.tmp	
Process:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.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:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp2F0A.tmp	
Process:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1603
Entropy (8bit):	5.140428833613153
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtnHxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTnRv
MD5:	636AB9BAC6C169CDFF479FC4A8B5B2DC
SHA1:	A442D14DF6A336942CD7951BEC11E92A5BD41318
SHA-256:	78925356A9CC22EE1B162CB30D1873E342256A56D5FD798215E878E754E782A1
SHA-512:	6FBA4FCEF103183B95FFA893A78A50BBF41BF2C522C2FCF612A94709185589A43EC6693990C88D40FB06342B7BC116A8FD2408FBD122CE2B31160D74D30DB9F
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <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\tmp3D43.tmp	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1603
Entropy (8bit):	5.140428833613153
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtnHxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTnRv
MD5:	636AB9BAC6C169CDFF479FC4A8B5B2DC
SHA1:	A442D14DF6A336942CD7951BEC11E92A5BD41318
SHA-256:	78925356A9CC22EE1B162CB30D1873E342256A56D5FD798215E878E754E782A1
SHA-512:	6FBA4FCEF103183B95FFA893A78A50BBF41BF2C522C2FCF612A94709185589A43EC6693990C88D40FB06342B7BC116A8FD2408FBD122CE2B31160D74D30DB9F
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <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\tmp6482.tmp	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1603
Entropy (8bit):	5.140428833613153
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtnHxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTnRv
MD5:	636AB9BAC6C169CDFF479FC4A8B5B2DC
SHA1:	A442D14DF6A336942CD7951BEC11E92A5BD41318
SHA-256:	78925356A9CC22EE1B162CB30D1873E342256A56D5FD798215E878E754E782A1
SHA-512:	6FBA4FCEF103183B95FFA893A78A50BBF41BF2C522C2FCF612A94709185589A43EC6693990C88D40FB06342B7BC116A8FD2408FBD122CE2B31160D74D30DB9F
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <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\tmpD11B.tmp	
Process:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1603
Entropy (8bit):	5.140428833613153
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtnHxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTnRv
MD5:	636AB9BAC6C169CDFF479FC4A8B5B2DC
SHA1:	A442D14DF6A336942CD7951BEC11E92A5BD41318
SHA-256:	78925356A9CC22EE1B162CB30D1873E342256A56D5FD798215E878E754E782A1
SHA-512:	6FBA4FCEF103183B95FFA893A78A50BBF41BF2C522C2FCF612A94709185589A43EC6693990C88D40FB06342B7BC116A8FD2408FBD122CE2B31160D74D30DB9F
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <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\tmpF941.tmp	
Process:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1306
Entropy (8bit):	5.124999360975329
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0P2xtn:cbk4oL600QydbQxIYODOLedq3S2j
MD5:	EB082279877F1AEC7D8266B852EE0E08
SHA1:	BDE9B4336C1D77F909D36CE4DCA0E1EDAAF3D22C
SHA-256:	747AFDCF420562FE50E1B00F42FA7196547D42E754F162DBA2256BBBA8E33561
SHA-512:	54B5EA7AC4884B31D36AAD73011B45DA02410591F71D0278E6BA7FE7AE2777E7657BE8B8053786AB93C9A5B951CFD9F979BDB3FFDC39F9713510A3AD01521245
Malicious:	false
Reputation:	unknown

Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

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

Process:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:xln:z
MD5:	6ECD96FF55617E76B86DFD3CD32E863B
SHA1:	285A3D47F2E6EB5EC7B2820C7CB5E898FE3F21A6
SHA-256:	28A946F3E7956E4EB4B232AE02362A776CD8A0A60A6A52405BB3ACCE69CAAC42
SHA-512:	4AE2F92F9CC16E6348669A52E56AC129E6AD78402587CE9215BCA7155DF5C820574D2DC3E0C2B5595F63DC805989DFD0C1B859C56F1A251AE416D25644CADAE
Malicious:	**true**
Reputation:	unknown
Preview:	..W.o3.H

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

Process:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	43
Entropy (8bit):	4.68207870819047
Encrypted:	false
SSDEEP:	3:oNUWJRWdTipLg0Cn:oNNJAgpU0C
MD5:	243D3F1C3EDF82240704FDD7E840B52D
SHA1:	43391CC35F31B2301B3F30132AB28318E8B2FDFB
SHA-256:	2EFCE0AAA835ECB29BF2477B231FE897F83A3C9525DAC08D990D8F0174A47D4D
SHA-512:	E06BFED1EFDA8BED7F724B37EC70803FF4F3921FA0A46E77E784B99B5E617F4C7A15A202AEC59B45242D7CA4201F7EE0FEE0680019F16AA11C059BF23325551D
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe

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

Process:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	721408
Entropy (8bit):	7.8544731914193955
Encrypted:	false
SSDEEP:	12288:W0jBpXpjRAatpjiaPJxDWU/Lh7NUfMbMFEXgqA8LMPYdwo+/jJHYtop:XjBtj2aPJ1/hN5bVwbqMQdh+/1Yto
MD5:	A2BB923C86585AAA72A8858FB84CBC22
SHA1:	B6404ADBE754315915EF021CA73309CBB4BA9EA7
SHA-256:	22ACE1DA7A25D7597434CC2EC2568A5F3E4C6CFD018FBA8251E7273340BE3DE2
SHA-512:	A194B247403D4F854698D89A3A13F43D77A15744B407C3F53C66F12CF3E82553077C51930A80D28FA5E8A5EFEB02CC4DD8920A304696049F24BB59AD8F57969D
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....\{b.....0.....Z..... .....@.. .....`..... ..@.....K.....W.....@.....e..... ..... ..H.....text..... ..... ..`.rsrc....W.....X.....@..@.reloc.....@.....@..B.....H.....@.....b(....8.....(....8.....*....(....8.....(....8.....(....8....*.^(.....(.....(.....*.{....*6..}....8....*...0.....(.....8.....*.....(.....*.0..%.....8....8....8.....(....(...+..8.....*.....{....*"..}....*....0..._.....8.....*8....8....r...p.(.....(....r...p.(.....:.....8.....o....(.....8.....0.....(.....8.....*..{....*"..}....*...&~.....*...~..

C:\Users\user\AppData\Roaming\DizKUzcAmYAC.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 E
Malicious:	false
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220511\PowerShell_transcript.045012.Eo625rMf.20220511095527.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):	5807
Entropy (8bit):	5.405180104196973
Encrypted:	false
SSDEEP:	96:BZx/wNNqDo1ZSZ//wNNqDo1ZEsKkjZg/wNNqDo1Z7N00IZn:l
MD5:	8AC61ABE78054330B788950499789AFF
SHA1:	889DB7255684D0297AAB0019C147A38AC9DE62A9
SHA-256:	7458DC37512C334371D09BA15AE6876005B932CA91B1587C54FD4DBE9FB30FFE
SHA-512:	9BDAE3672AA5040C00005CD6B1254984D6D57ADCBD5698E3011A4C1F0D4CE5B17F172C25D12EF4DDDBA668501FA928BE15CC1EED74AFBED20846E5AADAC3 D18A
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220511095529..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 045012 (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\DizKUzcAmYAC.exe..Process ID: 4356..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: 20220511095529..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppD ata\Roaming\DizKUzcAmYAC.exe..**********..Windows PowerShell transcript start..Start time: 20220511095912..Username: computer\user..RunAs User: DESK TOP-716

C:\Users\user\Documents\20220511\PowerShell_transcript.045012.aOio_RNq.20220511095551.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):	5807
Entropy (8bit):	5.40529914172891
Encrypted:	false
SSDEEP:	96:BZg/wNWqDo1ZNZU/wNWqDo1ZgsKkjZyG/wNWqDo1ZfN00BZO:Y5
MD5:	FAEC881C1A92534A70D3B7999D492B23
SHA1:	07B6CD91C0F2E0C4FF3881DC6C3EE4E29C7C00FD
SHA-256:	BC24763FC0E85CE80DF15A843AE457422C87AA765470A3DEE1A43A206AFCF980
SHA-512:	EC0F674F10006379F0E3EE51A996A0B01BC19F834E70150580BA4EE45DE64068B99F69E60770B80E821564ED856646D5ACB20B27E3EDA39E7143762E7108BB96
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220511095553..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 045012 (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\DizKUzcAmYAC.exe..Process ID: 4456..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: 20220511095553..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppD ata\Roaming\DizKUzcAmYAC.exe..**********..Windows PowerShell transcript start..Start time: 20220511095908..Username: computer\user..RunAs User: DESK TOP-716

C:\Users\user\Documents\20220511\PowerShell_transcript.045012.nodeFhPp.20220511095555.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):	5807
Entropy (8bit):	5.4026101642199205
Encrypted:	false
SSDEEP:	96:BZZ/wNzqDo1ZOZz/wNzqDo1ZasKkjZk/wNzqDo1ZaN00XXjZ9Xa:xra
MD5:	4B54D7A3ED54B7EF3D5450ECA4B9875F
SHA1:	7A5B032359864B2B80608B5565CA8DE3F752E8A8
SHA-256:	E4E6D06B77FB243DCFA5D929FCB1A6F064806B8C7BECF541D32CF5003CFCBAD9
SHA-512:	E318811660A86518F05D1C369541498118E563A11DE1E7BAC35C5C4D56B6D4C40B5578747C8087F0D19BDB3EB1BE9FCED08BE5BC769E7EE2E87A0264852F6DC
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220511095558..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 045012 (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\DizKUzcAmYAC.exe..Process ID: 4004..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: 20220511095558..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\DizKUzcAmYAC.exe..**********..Windows PowerShell transcript start..Start time: 20220511095916..Username: computer\user..RunAs User: DESKTOP-716

C:\Users\user\Documents\20220511\PowerShell_transcript.045012.p+Aoxp71.20220511095606.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):	5807
Entropy (8bit):	5.395900201776116
Encrypted:	false
SSDEEP:	96:BZy/wNKqDo1Z/ZU/wNKqDo1ZpsKkjZr/wNKqDo1ZhN00dZq:z
MD5:	676ED2B5C9C1B80E9E454C84279DC04E
SHA1:	04F3265039F08BA099DB23A305758E2930B8BAC1
SHA-256:	8DD7A38AFC68D7E39AE6FF6D35AD1226A8032DDABA71C64CE4F6E769AA110FC5
SHA-512:	8BEB4D11FD128E46123E6B49055DDEA02961E489358ECD4756ED5335E05AC587A080C437820B0AD1366FBDEF9552D4A9E61A02BCA51A3B34AE5C4BFBB1E97EC7
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220511095609..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 045012 (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\DizKUzcAmYAC.exe..Process ID: 5280..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: 20220511095609..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\DizKUzcAmYAC.exe..**********..Windows PowerShell transcript start..Start time: 20220511100022..Username: computer\user..RunAs User: DESKTOP-716

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8544731914193955
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • 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% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	8v2E2Qu0iMFG7kx.exe
File size:	721408
MD5:	a2bb923c86585aaa72a8858fb84cbc22
SHA1:	b6404adbe754315915ef021ca73309cbb4ba9ea7
SHA256:	22ace1da7a25d7597434cc2ec2568a5f3e4c6cfd018fba8251e7273340be3de2
SHA512:	a194b247403d4f854698d89a3a13f43d77a15744b407c3f53c66f12cf3e82553077c51930a80d28fa5e8a5efeb02cc4dd8920a304696049f24bb59ad8f57969d

SSDEEP:	12288:W0jBpXpjRAatpjiaPJxDWU/Lh7NUfMbMFEXgqA8LMPYdwo+/jJHYtop:XjBtj2aPJ1l/hN5bVwbqMQdh+/1Yto
TLSH:	57E40219ABEAC621E17D2F7FD4F251141778BE89A036E30E68C8224E5E137970E81797
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....\{b..............0......Z........... ....@.. ....`............@................................

File Icon

Icon Hash:	f0f2f25944bcce78

Static PE Info

General

Entrypoint:	0x4ac3fe
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x627B5C09 [Wed May 11 06:47:37 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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
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	0xac3b0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xae000	0x57cc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xac365	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	0xaa404	0xaa600	False	0.889032981016	data	7.85666121858	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xae000	0x57cc	0x5800	False	0.964932528409	data	7.89116200924	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb4000	0xc	0x200	False	0.041015625	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xae130	0x5164	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xb3294	0x14	data		
RT_VERSION	0xb32a8	0x338	data		
RT_MANIFEST	0xb35e0	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

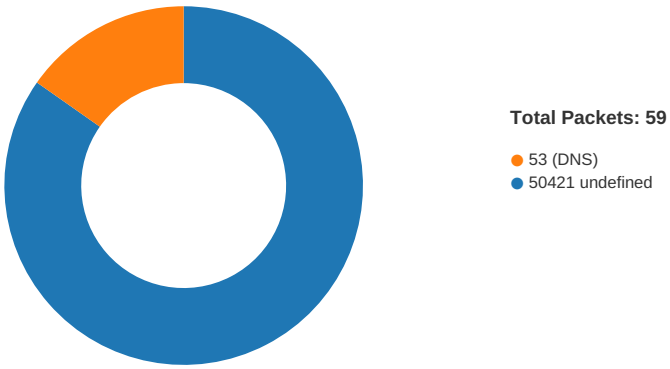
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Kids Mart 2012
Assembly Version	1.0.0.0
InternalName	LocalVariableI.exe
FileVersion	1.0.0.0
CompanyName	Kids Mart
LegalTrademarks	
Comments	
ProductName	Voroni
ProductVersion	1.0.0.0
FileDescription	Voroni
OriginalFilename	LocalVariableI.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2022 09:55:42.895190954 CEST	49779	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:55:43.122075081 CEST	50421	49779	185.19.85.175	192.168.2.5
May 11, 2022 09:55:43.715269089 CEST	49779	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:55:43.913105965 CEST	50421	49779	185.19.85.175	192.168.2.5
May 11, 2022 09:55:44.436619043 CEST	49779	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:55:44.674958944 CEST	50421	49779	185.19.85.175	192.168.2.5
May 11, 2022 09:55:48.991769075 CEST	49784	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:55:49.210901022 CEST	50421	49784	185.19.85.175	192.168.2.5
May 11, 2022 09:55:49.871958017 CEST	49784	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:55:50.069803953 CEST	50421	49784	185.19.85.175	192.168.2.5
May 11, 2022 09:55:50.575187922 CEST	49784	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:55:50.775223017 CEST	50421	49784	185.19.85.175	192.168.2.5
May 11, 2022 09:55:54.861179113 CEST	49786	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:55:55.063085079 CEST	50421	49786	185.19.85.175	192.168.2.5
May 11, 2022 09:55:55.716295958 CEST	49786	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:55:55.910480022 CEST	50421	49786	185.19.85.175	192.168.2.5
May 11, 2022 09:55:56.528731108 CEST	49786	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:55:56.732714891 CEST	50421	49786	185.19.85.175	192.168.2.5
May 11, 2022 09:56:01.225589991 CEST	49790	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:01.477992058 CEST	50421	49790	185.19.85.175	192.168.2.5
May 11, 2022 09:56:02.029179096 CEST	49790	50421	192.168.2.5	185.19.85.175

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2022 09:56:02.268254042 CEST	50421	49790	185.19.85.175	192.168.2.5
May 11, 2022 09:56:02.826195955 CEST	49790	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:03.063239098 CEST	50421	49790	185.19.85.175	192.168.2.5
May 11, 2022 09:56:08.031821012 CEST	49792	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:08.282731056 CEST	50421	49792	185.19.85.175	192.168.2.5
May 11, 2022 09:56:08.822079897 CEST	49792	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:09.044785976 CEST	50421	49792	185.19.85.175	192.168.2.5
May 11, 2022 09:56:09.631428957 CEST	49792	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:09.852361917 CEST	50421	49792	185.19.85.175	192.168.2.5
May 11, 2022 09:56:13.950690031 CEST	49795	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:14.184129953 CEST	50421	49795	185.19.85.175	192.168.2.5
May 11, 2022 09:56:14.817750931 CEST	49795	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:15.038367033 CEST	50421	49795	185.19.85.175	192.168.2.5
May 11, 2022 09:56:15.627948046 CEST	49795	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:15.844495058 CEST	50421	49795	185.19.85.175	192.168.2.5
May 11, 2022 09:56:20.141938925 CEST	49796	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:20.361229897 CEST	50421	49796	185.19.85.175	192.168.2.5
May 11, 2022 09:56:20.925443888 CEST	49796	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:21.135596991 CEST	50421	49796	185.19.85.175	192.168.2.5
May 11, 2022 09:56:21.737888098 CEST	49796	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:21.945067883 CEST	50421	49796	185.19.85.175	192.168.2.5
May 11, 2022 09:56:26.164182901 CEST	49799	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:26.417016983 CEST	50421	49799	185.19.85.175	192.168.2.5
May 11, 2022 09:56:26.925801992 CEST	49799	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:27.156704903 CEST	50421	49799	185.19.85.175	192.168.2.5
May 11, 2022 09:56:27.816521883 CEST	49799	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:28.010056973 CEST	50421	49799	185.19.85.175	192.168.2.5
May 11, 2022 09:56:32.089411020 CEST	49806	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:32.311283112 CEST	50421	49806	185.19.85.175	192.168.2.5
May 11, 2022 09:56:32.816972971 CEST	49806	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:33.032269001 CEST	50421	49806	185.19.85.175	192.168.2.5
May 11, 2022 09:56:33.535701036 CEST	49806	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:33.774082899 CEST	50421	49806	185.19.85.175	192.168.2.5
May 11, 2022 09:56:37.787563086 CEST	49807	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:38.019655943 CEST	50421	49807	185.19.85.175	192.168.2.5
May 11, 2022 09:56:38.520545006 CEST	49807	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:38.725164890 CEST	50421	49807	185.19.85.175	192.168.2.5
May 11, 2022 09:56:39.411250114 CEST	49807	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:39.634567022 CEST	50421	49807	185.19.85.175	192.168.2.5
May 11, 2022 09:56:43.751183033 CEST	49810	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:43.966969967 CEST	50421	49810	185.19.85.175	192.168.2.5
May 11, 2022 09:56:44.555167913 CEST	49810	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:44.772430897 CEST	50421	49810	185.19.85.175	192.168.2.5
May 11, 2022 09:56:45.302359104 CEST	49810	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:45.491163969 CEST	50421	49810	185.19.85.175	192.168.2.5
May 11, 2022 09:56:49.506967068 CEST	49812	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:49.695203066 CEST	50421	49812	185.19.85.175	192.168.2.5
May 11, 2022 09:56:50.271513939 CEST	49812	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:50.460344076 CEST	50421	49812	185.19.85.175	192.168.2.5
May 11, 2022 09:56:50.974719048 CEST	49812	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:51.206366062 CEST	50421	49812	185.19.85.175	192.168.2.5
May 11, 2022 09:56:55.267849922 CEST	49814	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:55.473612070 CEST	50421	49814	185.19.85.175	192.168.2.5
May 11, 2022 09:56:55.975163937 CEST	49814	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:56.188702106 CEST	50421	49814	185.19.85.175	192.168.2.5
May 11, 2022 09:56:56.693973064 CEST	49814	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:56:56.905783892 CEST	50421	49814	185.19.85.175	192.168.2.5
May 11, 2022 09:57:01.648294926 CEST	49816	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:57:01.901226997 CEST	50421	49816	185.19.85.175	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2022 09:57:02.538203001 CEST	49816	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:57:02.752525091 CEST	50421	49816	185.19.85.175	192.168.2.5
May 11, 2022 09:57:03.335119963 CEST	49816	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:57:03.561134100 CEST	50421	49816	185.19.85.175	192.168.2.5
May 11, 2022 09:57:07.625297070 CEST	49840	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:57:07.842431068 CEST	50421	49840	185.19.85.175	192.168.2.5
May 11, 2022 09:57:08.351253986 CEST	49840	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:57:08.581243038 CEST	50421	49840	185.19.85.175	192.168.2.5
May 11, 2022 09:57:09.085596085 CEST	49840	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:57:09.329368114 CEST	50421	49840	185.19.85.175	192.168.2.5
May 11, 2022 09:57:13.342575073 CEST	49863	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:57:13.565594912 CEST	50421	49863	185.19.85.175	192.168.2.5
May 11, 2022 09:57:14.070599079 CEST	49863	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:57:14.290539980 CEST	50421	49863	185.19.85.175	192.168.2.5
May 11, 2022 09:57:14.804891109 CEST	49863	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:57:15.008971930 CEST	50421	49863	185.19.85.175	192.168.2.5
May 11, 2022 09:57:19.056550026 CEST	49871	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:57:19.264847040 CEST	50421	49871	185.19.85.175	192.168.2.5
May 11, 2022 09:57:19.867783070 CEST	49871	50421	192.168.2.5	185.19.85.175
May 11, 2022 09:57:20.089411974 CEST	50421	49871	185.19.85.175	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2022 09:55:42.861223936 CEST	63187	53	192.168.2.5	8.8.8.8
May 11, 2022 09:55:42.882559061 CEST	53	63187	8.8.8.8	192.168.2.5
May 11, 2022 09:55:48.970916986 CEST	52982	53	192.168.2.5	8.8.8.8
May 11, 2022 09:55:48.990214109 CEST	53	52982	8.8.8.8	192.168.2.5
May 11, 2022 09:55:54.816165924 CEST	57352	53	192.168.2.5	8.8.8.8
May 11, 2022 09:55:54.836055040 CEST	53	57352	8.8.8.8	192.168.2.5
May 11, 2022 09:56:20.115586996 CEST	55355	53	192.168.2.5	8.8.8.8
May 11, 2022 09:56:20.138335943 CEST	53	55355	8.8.8.8	192.168.2.5
May 11, 2022 09:56:26.011401892 CEST	49407	53	192.168.2.5	8.8.8.8
May 11, 2022 09:56:26.028888941 CEST	53	49407	8.8.8.8	192.168.2.5
May 11, 2022 09:56:32.066603899 CEST	57990	53	192.168.2.5	8.8.8.8
May 11, 2022 09:56:32.085817099 CEST	53	57990	8.8.8.8	192.168.2.5
May 11, 2022 09:56:55.246997118 CEST	54463	53	192.168.2.5	8.8.8.8
May 11, 2022 09:56:55.266129017 CEST	53	54463	8.8.8.8	192.168.2.5
May 11, 2022 09:57:01.625391006 CEST	49416	53	192.168.2.5	8.8.8.8
May 11, 2022 09:57:01.646750927 CEST	53	49416	8.8.8.8	192.168.2.5
May 11, 2022 09:57:07.601516008 CEST	62706	53	192.168.2.5	8.8.8.8
May 11, 2022 09:57:07.623550892 CEST	53	62706	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 11, 2022 09:55:44.738735914 CEST	192.168.2.5	8.8.8.8	d09b	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 11, 2022 09:55:42.861223936 CEST	192.168.2.5	8.8.8.8	0x4b84	Standard query (0)	lowspeed121.ddns.net	A (IP address)	IN (0x0001)
May 11, 2022 09:55:48.970916986 CEST	192.168.2.5	8.8.8.8	0x6515	Standard query (0)	lowspeed121.ddns.net	A (IP address)	IN (0x0001)
May 11, 2022 09:55:54.816165924 CEST	192.168.2.5	8.8.8.8	0x9f87	Standard query (0)	lowspeed121.ddns.net	A (IP address)	IN (0x0001)
May 11, 2022 09:56:20.115586996 CEST	192.168.2.5	8.8.8.8	0x256c	Standard query (0)	lowspeed121.ddns.net	A (IP address)	IN (0x0001)
May 11, 2022 09:56:26.011401892 CEST	192.168.2.5	8.8.8.8	0x4f34	Standard query (0)	lowspeed121.ddns.net	A (IP address)	IN (0x0001)

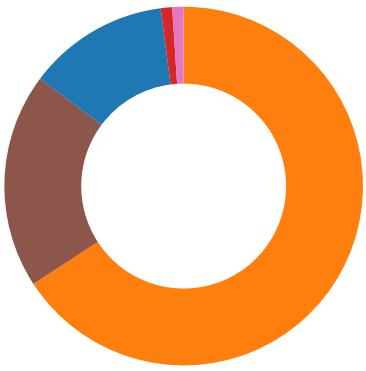
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 11, 2022 09:56:32.066603899 CEST	192.168.2.5	8.8.8.8	0xfca4	Standard query (0)	lowspeed12 1.ddns.net	A (IP address)	IN (0x0001)
May 11, 2022 09:56:55.246997118 CEST	192.168.2.5	8.8.8.8	0x3617	Standard query (0)	lowspeed12 1.ddns.net	A (IP address)	IN (0x0001)
May 11, 2022 09:57:01.625391006 CEST	192.168.2.5	8.8.8.8	0x58a6	Standard query (0)	lowspeed12 1.ddns.net	A (IP address)	IN (0x0001)
May 11, 2022 09:57:07.601516008 CEST	192.168.2.5	8.8.8.8	0xbd2f	Standard query (0)	lowspeed12 1.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2022 09:55:42.882559061 CEST	8.8.8.8	192.168.2.5	0x4b84	No error (0)	lowspeed12 1.ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
May 11, 2022 09:55:48.990214109 CEST	8.8.8.8	192.168.2.5	0x6515	No error (0)	lowspeed12 1.ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
May 11, 2022 09:55:54.836055040 CEST	8.8.8.8	192.168.2.5	0x9f87	No error (0)	lowspeed12 1.ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
May 11, 2022 09:56:20.138335943 CEST	8.8.8.8	192.168.2.5	0x256c	No error (0)	lowspeed12 1.ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
May 11, 2022 09:56:26.028888941 CEST	8.8.8.8	192.168.2.5	0x4f34	No error (0)	lowspeed12 1.ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
May 11, 2022 09:56:32.085817099 CEST	8.8.8.8	192.168.2.5	0xfca4	No error (0)	lowspeed12 1.ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
May 11, 2022 09:56:55.266129017 CEST	8.8.8.8	192.168.2.5	0x3617	No error (0)	lowspeed12 1.ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
May 11, 2022 09:57:01.646750927 CEST	8.8.8.8	192.168.2.5	0x58a6	No error (0)	lowspeed12 1.ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
May 11, 2022 09:57:07.623550892 CEST	8.8.8.8	192.168.2.5	0xbd2f	No error (0)	lowspeed12 1.ddns.net		185.19.85.175	A (IP address)	IN (0x0001)

Statistics

Behavior



- 8v2E2Qu0iMFG7kx.exe
- powershell.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- 8v2E2Qu0iMFG7kx.exe
- schtasks.exe
- conhost.exe
- schtasks.exe
- 8v2E2Qu0iMFG7kx.exe
- conhost.exe
- dhcpmon.exe
- dhcpmon.exe
- powershell.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- powershell.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- 8v2E2Qu0iMFG7kx.exe
- dhcpmon.exe
- 8v2E2Qu0iMFG7kx.exe
- powershell.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- dhcpmon.exe
- dhcpmon.exe

Click to jump to process

System Behavior

Analysis Process: 8v2E2Qu0iMFG7kx.exe PID: 7112, Parent PID: 5968

General

Target ID:	0
Start time:	09:55:12
Start date:	11/05/2022
Path:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe"
Imagebase:	0x780000
File size:	721408 bytes
MD5 hash:	A2BB923C86585AAA72A8858FB84CBC22
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: 00000000.00000002.489972165.0000000002C21000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.491146282.0000000003D2F000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.491146282.0000000003D2F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.491146282.0000000003D2F000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.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	6E65CF06	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	6E65CF06	unknown
C:\Users\user\AppData\Roaming\DizKUzcAmYAC.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	6D5ADD66	CopyFileW
C:\Users\user\AppData\Roaming\DizKUzcAmYAC.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6D5ADD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpD11B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D5A7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8v2E2Qu0iMFG7kx.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E96C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD11B.tmp	success or wait	1	6D5A6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\DizKUzcAmYAC.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 09 5c 7b 62 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 30 00 00 fd 0a 00 00 5a 00 00 00 00 00 00 fd fd 0a 00 00 20 00 00 00 fd 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 0b 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL\{b0Z @ `@	success or wait	3	6D5ADD66	CopyFileW
C:\Users\user\AppData\Roaming\DizKUzcAmYAC.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	6D5ADD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpD11B.tmp	0	1603	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 61 6c 66 6f 6e 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	<?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	6D5A1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\8v2E2Qu0iMFG7kx.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	6E96C907	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	6E635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E635705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E63CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6E5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6E5903DE	ReadFile

Analysis Process: powershell.exe PID: **4356**, Parent PID: **7112**

General

Target ID:	4
Start time:	09:55:26
Start date:	11/05/2022
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\DizKUzcAmYAC.exe
Imagebase:	0xc80000
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	6E65CF06	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	6E65CF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ccwhzi4g.sgh.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D5A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_e2th3aur.tfw.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D5A1E60	CreateFileW
C:\Users\user\Documents\20220511	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D5ABEFF	CreateDirectoryW
C:\Users\user\Documents\20220511\PowerShell_transcript.045012.Eo625rMf.20220511095527.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D5A1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ccwhzi4g.sgh.ps1	success or wait	1	6D5A6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_e2th3aur.tfw.psm1	success or wait	1	6D5A6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_ccwhzi4g.sgh.ps1	0	1	31	1	success or wait	1	6D5A1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_e2th3aur.tfw.psm1	0	1	31	1	success or wait	1	6D5A1B4F	WriteFile
C:\Users\user\Documents\20220511\PowerShell_transcript.045012.Eo625rMf.20220511095527.txt	0	3	ff		success or wait	1	6D5A1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220511\PowerShell_transcript.045012.Eo625rMf.20220511095527.txt	3	682	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 31 31 30 39 35 35 32 39 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 61 6c 66 6f 6e 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 61 6c 66 6f 6e 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 30 34 35 30 31 32 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	**********************Windows PowerShell transcript startStart time: 20220511095529Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 045012 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\	success or wait	44	6D5A1B4F	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 64 14 00 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@ed	success or wait	1	6E9276FC	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	6E9276FC	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	6E9276FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6E9276FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6E9276FC	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 40 01 fd 44 40 01 6d 45 40 01 45 4d 40 01 fd 71 40 01 fd 71 40 01 fd 53 40 01 fd 25 40 01 fd 6e 40 01 34 26 40 01 35 26 40 01 37 26 40	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@BM@D@mE@EM@q@q@S@%@n@4&@5&@7&@	success or wait	11	6E9276FC	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	6E635705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E635705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E5903DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E63CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E63CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E63CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E5903DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E635705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E635705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E635705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E635705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E635705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E641F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23116	success or wait	1	6E64203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E5903DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6D5A1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6D5A1B4F	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	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E5903DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E635705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E635705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E635705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E635705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6D5A1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	15	6D5A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6D5A1B4F	ReadFile

Analysis Process: conhost.exe PID: **6468**, Parent PID: **4356**

General

Target ID:	5
Start time:	09:55:26
Start date:	11/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: **4384**, Parent PID: **7112**

General

Target ID:	6
Start time:	09:55:27
Start date:	11/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\DizKUzcAmYAC" /XML "C:\Users\user\AppData\Local\Temp\tmpD11B.tmp
Imagebase:	0xba0000
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\tmpD11B.tmp	unknown	2	success or wait	1	BAAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD11B.tmp	unknown	1604	success or wait	1	BAABD9	ReadFile

Analysis Process: conhost.exe PID: **5220**, Parent PID: **4384**

General	
Target ID:	7
Start time:	09:55:28
Start date:	11/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: 8v2E2Qu0iMFG7kx.exe PID: **3016**, Parent PID: **7112**

General	
Target ID:	8
Start time:	09:55:30
Start date:	11/05/2022
Path:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe
Imagebase:	0x900000
File size:	721408 bytes
MD5 hash:	A2BB923C86585AAA72A8858FB84CBC22
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: 00000008.00000000.486953208.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.486953208.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.486953208.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.715262668.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.715262668.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.715262668.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.722148226.00000000055D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.722148226.00000000055D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.722148226.00000000055D0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.486044015.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.486044015.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.486044015.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.722115639.00000000055B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.722115639.00000000055B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.722115639.00000000055B0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.718979964.0000000002D91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.722387671.0000000006560000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.722387671.0000000006560000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.722387671.0000000006560000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000008.00000002.722387671.0000000006560000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.720205321.0000000003DD9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.720205321.0000000003DD9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.483650905.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.483650905.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.483650905.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.484715785.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.484715785.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.484715785.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.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	6E65CF06	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	6E65CF06	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	6D5ABEFF	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	6D5A1E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D5ABEFF	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	6D5ADD66	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	6D5ADD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF941.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D5A7038	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	6D5A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp23B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D5A7038	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	6D5ABEFF	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	6D5ABEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF941.tmp	success or wait	1	6D5A6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp23B.tmp	success or wait	1	6D5A6A95	DeleteFileW
C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe:Zone.Identifier	success or wait	1	5358B06	DeleteFileA

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 57 11 6f 33 fd 48	Wo3H	success or wait	1	6D5A1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 09 5c 7b 62 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 30 00 00 fd 0a 00 00 5a 00 00 00 00 00 00 fd fd 0a 00 00 20 00 00 00 fd 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 0b 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL\{b0Z @ `@	success or wait	3	6D5ADD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6D5ADD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF941.tmp	0	1306	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	6D5A1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	43	43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 44 65 73 6b 74 6f 70 5c 38 76 32 45 32 51 75 30 69 4d 46 47 37 6b 78 2e 65 78 65	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe	success or wait	1	6D5A1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp23B.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	6D5A1B4F	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	6E635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E635705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E63CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E5903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E5903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E635705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D5A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D5A1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E61D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E61D72F	unknown
C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe	unknown	4096	success or wait	1	6E61D72F	unknown
C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe	unknown	512	success or wait	1	6E61D72F	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	6D5A646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **5132**, Parent PID: **3016**

General	
Target ID:	13
Start time:	09:55:37
Start date:	11/05/2022
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\tmpF941.tmp
Imagebase:	0xba0000
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\tmpF941.tmp	unknown	2	success or wait	1	BAAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF941.tmp	unknown	1307	success or wait	1	BAABD9	ReadFile

Analysis Process: conhost.exe PID: **4488**, Parent PID: **5132**

General	
Target ID:	14
Start time:	09:55:37
Start date:	11/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: **6388**, Parent PID: **3016**

General	
Target ID:	15
Start time:	09:55:39
Start date:	11/05/2022
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\tmp23B.tmp
Imagebase:	0xba0000
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: 8v2E2Qu0iMFG7kx.exe PID: **6564**, Parent PID: **1040**

General

Target ID:	16
Start time:	09:55:39
Start date:	11/05/2022
Path:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe 0
Imagebase:	0x1b0000
File size:	721408 bytes
MD5 hash:	A2BB923C86585AAA72A8858FB84CBC22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.586896158.000000000375F000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.586896158.000000000375F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.586896158.000000000375F000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000010.00000002.582094777.0000000002651000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: conhost.exe PID: **6172**, Parent PID: **6388**

General

Target ID:	17
Start time:	09:55:40
Start date:	11/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: **6708**, Parent PID: **1040**

General

Target ID:	18
Start time:	09:55:42
Start date:	11/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x830000
File size:	721408 bytes
MD5 hash:	A2BB923C86585AAA72A8858FB84CBC22
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: 00000012.00000002.577142457.0000000003E1F000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.577142457.0000000003E1F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.577142457.0000000003E1F000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000012.00000002.575971279.0000000002D11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: dhcpmon.exe PID: **5288**, Parent PID: **684**

General

Target ID:	20
Start time:	09:55:47
Start date:	11/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xe60000
File size:	721408 bytes
MD5 hash:	A2BB923C86585AAA72A8858FB84CBC22
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: 00000014.00000002.599492533.000000000432F000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.599492533.000000000432F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.599492533.000000000432F000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000014.00000002.596685149.0000000003221000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: powershell.exe PID: **4456**, Parent PID: **6564**

General

Target ID:	21
Start time:	09:55:50
Start date:	11/05/2022
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\DizKUzcAmYAC.exe
Imagebase:	0xc80000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: **3512**, Parent PID: **4456**

General

Target ID:	22
Start time:	09:55:50
Start date:	11/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: **2984**, Parent PID: **6564**

General

Target ID:	23
Start time:	09:55:51
Start date:	11/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\DizKUzcAmYAC" /XML "C:\Users\user\AppData\Local\Temp\tmp2F0A.tmp
Imagebase:	0xba0000
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: **5720**, Parent PID: **2984**

General

Target ID:	24
Start time:	09:55:52
Start date:	11/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: **4004**, Parent PID: **6708**

General

Target ID:	25
Start time:	09:55:54
Start date:	11/05/2022
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\DizKUzcAmYAC.exe
Imagebase:	0x7ff78ca80000
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: **4396**, Parent PID: **4004**

General	
Target ID:	26
Start time:	09:55:54
Start date:	11/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: **4448**, Parent PID: **6708**

General	
Target ID:	27
Start time:	09:55:55
Start date:	11/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\DizKUzcAmYAC" /XML "C:\Users\user\AppData\Local\Temp\tmp3D43.tmp
Imagebase:	0xba0000
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: **4536**, Parent PID: **4448**

General	
Target ID:	28
Start time:	09:55:57
Start date:	11/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 8v2E2Qu0iMFG7kx.exe PID: **4508**, Parent PID: **6564**

General	
Target ID:	29
Start time:	09:55:57

Start date:	11/05/2022
Path:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe
Imagebase:	0x100000
File size:	721408 bytes
MD5 hash:	A2BB923C86585AAA72A8858FB84CBC22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **4384**, Parent PID: **6708**

General

Target ID:	30
Start time:	09:55:59
Start date:	11/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xda0000
File size:	721408 bytes
MD5 hash:	A2BB923C86585AAA72A8858FB84CBC22
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: 0000001E.00000002.596653591.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.596653591.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.596653591.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001E.00000000.564181475.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000000.564181475.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000000.564181475.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001E.00000000.561622224.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000000.561622224.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000000.561622224.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001E.00000000.556903166.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000000.556903166.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000000.556903166.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001E.00000000.566406893.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000000.566406893.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000000.566406893.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.598741699.00000000031D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.598741699.00000000031D1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001E.00000002.599309950.00000000041D9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001E.00000002.599309950.00000000041D9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: 8v2E2Qu0iMFG7kx.exe PID: **6084**, Parent PID: **6564**

General

Target ID:	32
Start time:	09:56:00

Start date:	11/05/2022
Path:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\8v2E2Qu0iMFG7kx.exe
Imagebase:	0x550000
File size:	721408 bytes
MD5 hash:	A2BB923C86585AAA72A8858FB84CBC22
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: 00000020.00000002.605519664.0000000003989000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.605519664.0000000003989000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000020.00000000.567928899.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000000.567928899.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000000.567928899.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000002.605406624.0000000002981000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.605406624.0000000002981000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000020.00000002.604222168.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000002.604222168.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.604222168.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000020.00000000.576656186.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000000.576656186.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000000.576656186.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000020.00000000.571236527.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000000.571236527.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000000.571236527.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000020.00000000.573634029.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000000.573634029.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000000.573634029.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: powershell.exe PID: **5280**, Parent PID: **5288**

General

Target ID:	33
Start time:	09:56:04
Start date:	11/05/2022
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\DizKUzcAmYAC.exe
Imagebase:	0xc80000
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: **6020**, Parent PID: **5280**

General

Target ID:	34

Start time:	09:56:04
Start date:	11/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: **6440**, Parent PID: **5288**

General

Target ID:	36
Start time:	09:56:05
Start date:	11/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\DizKUzcAmYAC" /XML "C:\Users\user\AppData\Local\Temp\tmp6482.tmp
Imagebase:	0xba0000
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: **3240**, Parent PID: **6440**

General

Target ID:	37
Start time:	09:56:08
Start date:	11/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **7140**, Parent PID: **5288**

General

Target ID:	40
Start time:	09:56:12
Start date:	11/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x270000
File size:	721408 bytes
MD5 hash:	A2BB923C86585AAA72A8858FB84CBC22

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

Analysis Process: dhcpmon.exe PID: **6816**, Parent PID: **5288**

General

Target ID:	41
Start time:	09:56:15
Start date:	11/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xf60000
File size:	721408 bytes
MD5 hash:	A2BB923C86585AAA72A8858FB84CBC22
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: 00000029.00000000.585982290.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000029.00000000.585982290.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000029.00000000.585982290.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000029.00000000.591926047.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000029.00000000.591926047.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000029.00000000.591926047.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000029.00000002.613729837.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000029.00000002.613729837.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000029.00000002.613729837.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000029.00000000.592410825.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000029.00000000.592410825.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000029.00000000.592410825.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000029.00000002.615411010.00000000043C9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000029.00000002.615411010.00000000043C9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000029.00000000.591485124.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000029.00000000.591485124.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000029.00000000.591485124.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000029.00000002.615270098.00000000033C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000029.00000002.615270098.00000000033C1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

No disassembly