ID: 381644
Sample Name: wDIaJji4Vv.exe
Cookbook: default.jbs
Time: 02:35:32
Date: 04/04/2021
Version: 31.0.0 Emerald

Table of Contents

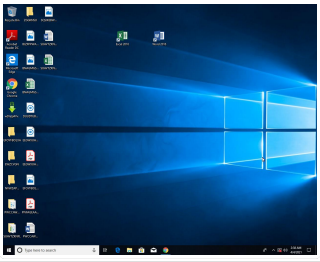
Analysis Report wDlaJji4Vv.exe

Overview

General Information

Sample Name:	wDlaJji4Vv.exe
Analysis ID:	381644
MD5:	6a0c22a8a8d952..
SHA1:	b75a74ca657f494.
SHA256:	cc9690dcde0dfa2..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

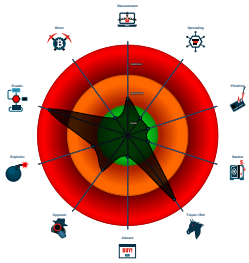
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Adds a directory exclusion to Windo…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…

Classification



Startup

- **System is w10x64**
- wDlaJji4Vv.exe (PID: 2788 cmdline: 'C:\Users\user\Desktop\wDlaJji4Vv.exe' MD5: 6A0C22A8A8D9524BA012910571B57D38)
  - powershell.exe (PID: 6104 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\wDlaJji4Vv.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 404 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 3120 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\LGKyjAEnmfdSo' /XML 'C:\Users\user\AppData\Local\Temp\tmpE049.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6100 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5528 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\LGKyjAEnmfdSo.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 4688 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - RegSvcs.exe (PID: 6172 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - RegSvcs.exe (PID: 6228 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 71369277D09DA0830C8C59F9E22BB23A)
- dhcpmon.exe (PID: 6744 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 6752 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "282cf72b-8a92-4c1b-b768-b591a1e0",
  "Group": "jobo",
  "Domain1": "james12.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 6060,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "",
  "BackupDNSServer": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.484889407.000000000688 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x59eb:$x1: NanoCore.ClientPluginHost • 0x5b48:$x2: IClientNetworkHost
0000000C.00000002.484889407.000000000688 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x59eb:$x2: NanoCore.ClientPluginHost • 0x6941:$s3: PipeExists • 0x5be1:$s4: PipeCreated • 0x5a05:$s5: IClientLoggingHost
0000000C.00000002.484797009.000000000684 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b0b:$x1: NanoCore.ClientPluginHost • 0x5b44:$x2: IClientNetworkHost
0000000C.00000002.484797009.000000000684 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5b0b:$x2: NanoCore.ClientPluginHost • 0x5c0f:$s4: PipeCreated • 0x5b25:$s5: IClientLoggingHost
00000000.00000002.221605771.000000000420 2000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x168295:$x1: NanoCore.ClientPluginHost • 0x19aab5:$x1: NanoCore.ClientPluginHost • 0x1682d2:$x2: IClientNetworkHost • 0x19aaf2:$x2: IClientNetworkHost • 0x16be05:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x19e625:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Click to see the 42 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.RegSvcs.exe.68b0000.28.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x3d99:$x1: NanoCore.ClientPluginHost • 0x3db3:$x2: IClientNetworkHost
12.2.RegSvcs.exe.68b0000.28.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x3d99:$x2: NanoCore.ClientPluginHost • 0x4dce:$s4: PipeCreated • 0x3d86:$s5: IClientLoggingHost
12.2.RegSvcs.exe.67c0000.21.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x6da5:$x1: NanoCore.ClientPluginHost • 0x6dd2:$x2: IClientNetworkHost
12.2.RegSvcs.exe.67c0000.21.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x6da5:$x2: NanoCore.ClientPluginHost • 0x7d74:$s2: FileCommand • 0xc776:$s4: PipeCreated • 0x6dbf:$s5: IClientLoggingHost
12.3.RegSvcs.exe.4a2a9ed.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x605:$x1: NanoCore.ClientPluginHost • 0x3bd6:$x1: NanoCore.ClientPluginHost • 0x63e:$x2: IClientNetworkHost

Click to see the 132 entries

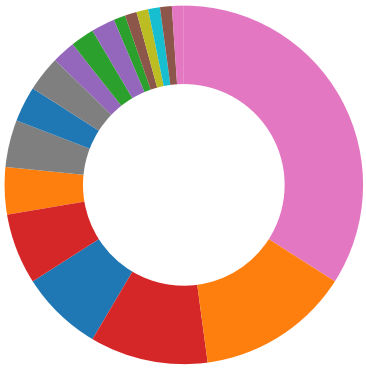
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

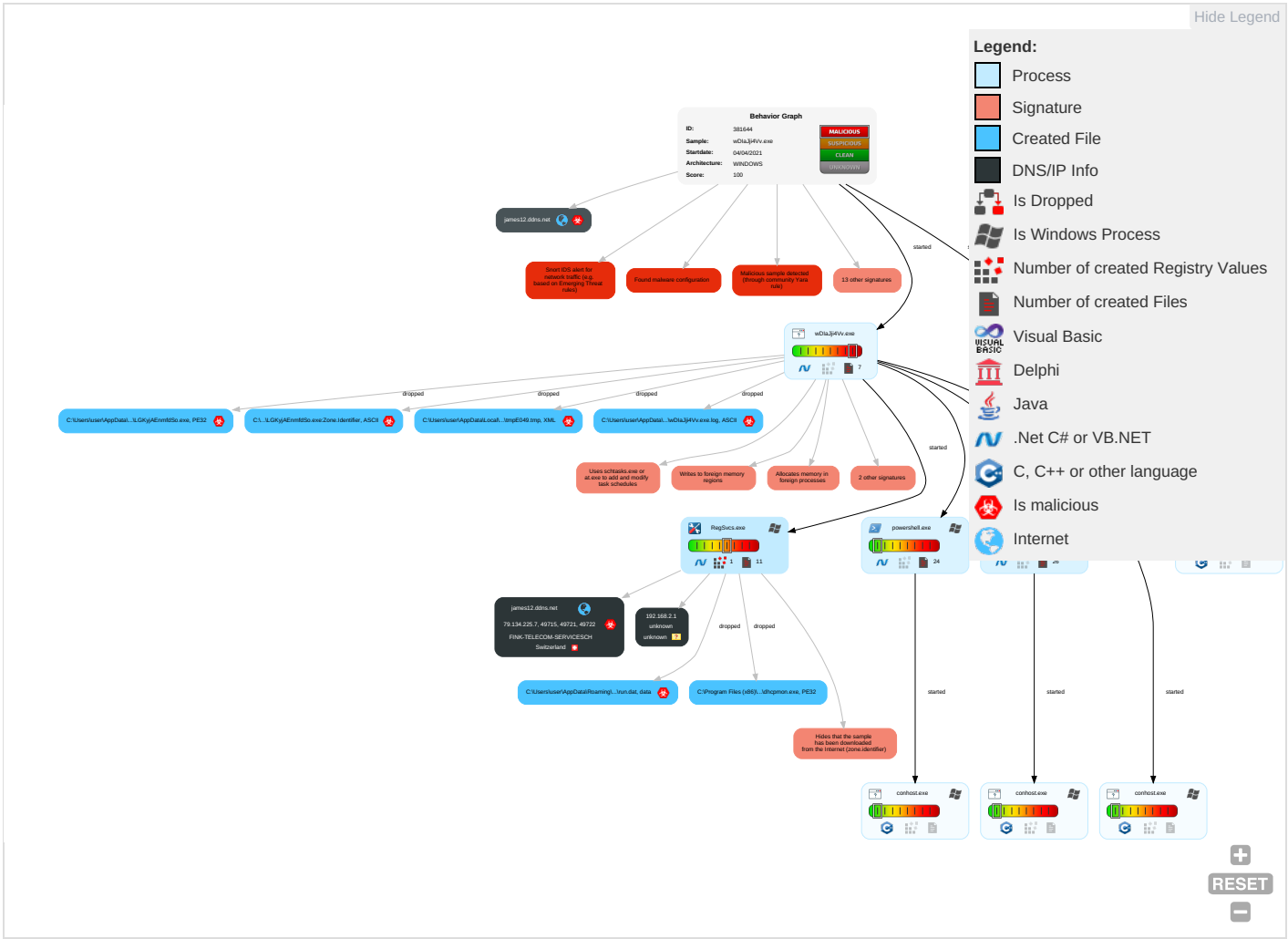
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1 1	Input Capture 2 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	E I N C
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 3	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Encrypted Channel 1	E F C
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 2	NTDS	Security Software Discovery 2 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 1	N D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 5 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 5 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 2 1	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	F A

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 3 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D I F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	F E

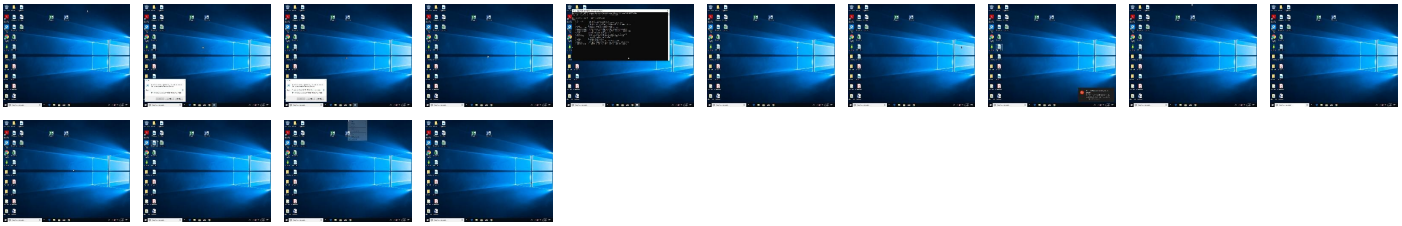
Behavior Graph



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
wDIaJji4Vv.exe	61%	Virustotal		Browse
wDIaJji4Vv.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
wDIaJji4Vv.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\LGKyjAEnmfdSo.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\LGKyjAEnmfdSo.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.2.RegSvcs.exe.5ec0000.18.unpack	100%	Avira	TR/NanoCore.fadte		Download File
12.2.RegSvcs.exe.4676f00.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
james12.ddns.net	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://go.microX%	0%	Avira URL Cloud	safe	
james12.ddns.net	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
james12.ddns.net	79.134.225.7	true	true	• 5%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
james12.ddns.net	true	• Avira URL Cloud: safe	unknown
127.0.0.1	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://go.microX%	powershell.exe, 00000002.00000003.278956963.00000000053E8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fileden.com/files/2011/10/5/3204996/curver.txt	wDIaJji4Vv.exe	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	wDIaJji4Vv.exe, 00000000.00000002.217455924.0000000003191000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.7	james12.ddns.net	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	381644
Start date:	04.04.2021
Start time:	02:35:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	wDIaJji4Vv.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:	40
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@18/19@18/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.4% (good quality ratio 3.1%) • Quality average: 76.6% • Quality standard deviation: 28.2%
HCA Information:	• Successful, ratio: 86% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
02:36:20	API Interceptor	2x Sleep call for process: wDIaJji4Vv.exe modified
02:36:26	API Interceptor	938x Sleep call for process: RegSvcs.exe modified
02:36:31	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
02:36:49	API Interceptor	75x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.7	hbvo9thTAX.exe	Get hash	malicious	Browse	
	IMG_110_63_078SWIFT.exe	Get hash	malicious	Browse	
	PO-290321 (Itakrom).pif.exe	Get hash	malicious	Browse	
	PURCHASE ORDER EXPORT0022355048 SCAN DOC _PDF.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.568.10707.exe	Get hash	malicious	Browse	
	PO_1012_678_91.exe	Get hash	malicious	Browse	
	PO_1012_678_91.doc	Get hash	malicious	Browse	
	DrECSIMeTu.exe	Get hash	malicious	Browse	
	PI_061_Scanned_02.exe	Get hash	malicious	Browse	
	Transacion_CUS_REF_referencia es 000008223084566.vbe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
james12.ddns.net	hbvo9thTAX.exe	Get hash	malicious	Browse	• 79.134.225.7
	PURCHASE ORDER EXPORT0022355048 SCAN DOC _PDF.exe	Get hash	malicious	Browse	• 79.134.225.7

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	DkZY1k3y9F.exe	Get hash	malicious	Browse	• 79.134.225.23
	hbvo9thTAX.exe	Get hash	malicious	Browse	• 79.134.225.7
	SCAN ORDER DOC 040202021.exe	Get hash	malicious	Browse	• 79.134.225.71
	Waybill Doc_pdf.exe	Get hash	malicious	Browse	• 79.134.225.92
	gfcYixSdyD.exe	Get hash	malicious	Browse	• 79.134.225.71
	cJtVGjtNGZ.exe	Get hash	malicious	Browse	• 79.134.225.40
	Transferwise beneficiary detailspdf.exe	Get hash	malicious	Browse	• 79.134.225.22
	NS 001 DOP IPS ORIENTATIONS.doc	Get hash	malicious	Browse	• 79.134.225.73
	cp.msi.exe	Get hash	malicious	Browse	• 79.134.225.109
	ot.msi	Get hash	malicious	Browse	• 79.134.225.109
	dd.exe	Get hash	malicious	Browse	• 79.134.225.109
	IMG_110_63_078SWIFT.exe	Get hash	malicious	Browse	• 79.134.225.7
	yQY73z6zaP.exe	Get hash	malicious	Browse	• 79.134.225.25
	SOA6058.exe	Get hash	malicious	Browse	• 79.134.225.79
	PO-290321 (Itakrom).pif.exe	Get hash	malicious	Browse	• 79.134.225.7
	RFQ234.exe	Get hash	malicious	Browse	• 79.134.225.124
	EUjk8F87b8.exe	Get hash	malicious	Browse	• 79.134.225.82
	rgGyG2iLnd.exe	Get hash	malicious	Browse	• 79.134.225.22
	SCN-PV21-00920 P NEW ORDER.exe	Get hash	malicious	Browse	• 79.134.225.23
	jnHnxgMde8.exe	Get hash	malicious	Browse	• 79.134.225.54

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	cJtVGjtNGZ.exe	Get hash	malicious	Browse	
	Bilansno placanje.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Inject4.9647.20479.exe	Get hash	malicious	Browse	
	wnIPBdB5OF.exe	Get hash	malicious	Browse	
	Delivery Form C.exe	Get hash	malicious	Browse	
	h6uc8EaDQX.exe	Get hash	malicious	Browse	
	3aDHivUqWtumbXb.exe	Get hash	malicious	Browse	
	fMy120EQiT6NaRd.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Bulz.394792.29952.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.578.18498.exe	Get hash	malicious	Browse	
	sfTZCyMKuC.exe	Get hash	malicious	Browse	
	y9Rtu1cnBk.exe	Get hash	malicious	Browse	
	Ixli7b5j6A.exe	Get hash	malicious	Browse	
	nq0aCrCXyE.exe	Get hash	malicious	Browse	
	73SriHObnQ.exe	Get hash	malicious	Browse	
	0672IMP000158021.pdf.exe	Get hash	malicious	Browse	
	rb86llCYzA.exe	Get hash	malicious	Browse	
	C3GWn5tduT.exe	Get hash	malicious	Browse	
	uB8OTxUd3O.exe	Get hash	malicious	Browse	
	NNb2NBgsob.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.7515815714465193
Encrypted:	false
SSDEEP:	384:BOj9Y8/gS7SDriLGKq1MHR5U4Ag6ihJSxUCR1rgCPKabK2t0X5P7DZ+JgWSW72uw:B+gSAdN1MH3HAFRJngW2u
MD5:	71369277D09DA0830C8C59F9E22BB23A
SHA1:	37F9781314F0F6B7E9CB529A573F2B1C8DE9E93F
SHA-256:	D4527B7AD2FC4778CC5BE8709C95AEA44EAC0568B367EE14F7357D72898C3698
SHA-512:	2F470383E3C796C4CF212EC280854DBB9E7E8C8010CE6857E58F8E7066D7516B7CD7039BC5C0F547E1F5C7F9F2287869ADFFB2869800B08B2982A88BE96E9FB7
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: cJtVGjtNGZ.exe, Detection: malicious, Browse • Filename: Bilansno placanje.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Inject4.9647.20479.exe, Detection: malicious, Browse • Filename: wnIPBdB5OF.exe, Detection: malicious, Browse • Filename: Delivery Form C.exe, Detection: malicious, Browse • Filename: h6uc8EaDQX.exe, Detection: malicious, Browse • Filename: 3aDHivUqWtumbXb.exe, Detection: malicious, Browse • Filename: fMy120EQiT6NaRd.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Variant.Bulz.394792.29952.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.578.18498.exe, Detection: malicious, Browse • Filename: sfTZCyMKuC.exe, Detection: malicious, Browse • Filename: y9Rtu1cnBk.exe, Detection: malicious, Browse • Filename: Ixli7b5j6A.exe, Detection: malicious, Browse • Filename: nq0aCrCXyE.exe, Detection: malicious, Browse • Filename: 73SriHObnQ.exe, Detection: malicious, Browse • Filename: 0672IMP000158021.pdf.exe, Detection: malicious, Browse • Filename: rb86llCYzA.exe, Detection: malicious, Browse • Filename: C3GWn5tduT.exe, Detection: malicious, Browse • Filename: uB8OTxUd3O.exe, Detection: malicious, Browse • Filename: NNb2NBgsob.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{Z.....P... .....k.. .....@.. .....[.. ..@.....k..K..... k..... ....H.....text....K... ...P..... ..`.rsrc.....`.....@..@.rel oc.....p.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	5.016405576253028
Encrypted:	false
SSDEEP:	3:QHXMKaoWglAFXMWA2yTMGfsbNXLVd49Am12MFuAvOAsDeieVyn:Q3LawlAFXMWTyAGCFLIP12MUAvvrs
MD5:	50DEC1858E13F033E6DCA3CBFAD5E8DE
SHA1:	79AE1E9131B0FAF215B499D2F7B4C595AA120925
SHA-256:	14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4
SHA-512:	1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\wDlaJji4Vv.exe.log	
Process:	C:\Users\user\Desktop\wDlaJji4Vv.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages _v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Wind ows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\3577 4dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Size (bytes):	22300
Entropy (8bit):	5.351338582008221
Encrypted:	false
SSDEEP:	384:0tCDZ5SQAlOwksxQPrSrnSZI1JNc7nudTdvHhsVq1dOE7RC:95cZ3aPrynFXSbud7sQFc
MD5:	69E02A7CA4B49DD401027C43EA3ACC33
SHA1:	F12DA082F50DEA4D52E2A0E795DC9757A66795AE
SHA-256:	ED48047BF46291E5BE1F04F40F4949D320D3AC9E05E28041D75D5094AD7550E5
SHA-512:	D9D2EBDB4247DDD9DED1B4C1192B9DEE25F9D022F8C5EF211F5F1B29AB88A0BE29E6E2F1C3A14E018819ED3C88A16A82EF7B7C95F0C6BF5CDC4D0BC755DE6894
Malicious:	false
Preview:	@...e.....<.4.....@.....D.....fZve...F.....x.).....System.Management.AutomationH.....<@.^.L."My...:P..... .Microsoft.PowerShell .ConsoleHost4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_bn2wvdhj.h2i.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(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jbmpopxb.30w.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(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wlk4xu4b.yrc.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(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_z5wqclte.tm2.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(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmpE049.tmp	
Process:	C:\Users\user\Desktop\wDIaJji4Vv.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.193316411176685
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBttn:cbh47TlNQ//rydbz9I3YODOLNdq3Z
MD5:	81475B9DC7593991EC02E6E7BE2610AF
SHA1:	46FA27E643B1B7D0358398E47EEBE108FC111872
SHA-256:	9B514DA0E0BA2C415F45017C7EBC71FFF68D2E558AB0752F5C4A696B77D48320
SHA-512:	DDD9275E0B3108CF8B941296158BE6FEA8A0CCC6894518A5280FCD9DCFC596C50FAB0F467D7740C6EB3CD086B124E840FB72D09CA5AFF74DE9E0547E0ED56BE
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	2320
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwh:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCr
MD5:	0FBED11864C03FDED0E70014DCF84578
SHA1:	453723D938A03252F705B0A104986FE4C5CA7056
SHA-256:	70F5E49EE3091777827ED661B63842061220C899A708860986E9AA1BD87C5004
SHA-512:	DB53E3F1D18171F1D86C1B9BBF6BBD07153FC3E561834A35834BC0CA1E034FEDCD83AAAE7EDF9262C4E175C3D2287B647F55282E49627EAAF587F4371420466
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:1Ft:1Ft
MD5:	34A1E800A67FCD879983F01E669778C6
SHA1:	95BE704EB2AB8143FFDF4CFA5C395FA3798D264B

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SHA-256:	8EC741E0A64410932F16F47683C066DB038F3864F3D9A4FE670F9A57257A88E4
SHA-512:	478723D86A09BCC4A1A882E7DB8C23A85FEE3ADC26258A541DCD70DFC664CA883BA5C54E6996EBB6634EDCDFCE4AA273EFB04E305E459C29BF08C2C66BE8F14
Malicious:	**true**
Preview:	....M..H

C:\Users\user\AppData\Roaming\LGKyjAEnmfdSo.exe	
Process:	C:\Users\user\Desktop\wDIaJji4Vv.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	663040
Entropy (8bit):	7.081468136241616
Encrypted:	false
SSDEEP:	12288:7XAH590sYmLTYUxkaMjOXB7jreGkclqR:y0sYmZxfMKXBXreGk8
MD5:	6A0C22A8A8D9524BA012910571B57D38
SHA1:	B75A74CA657F4940B251C5116BCF2D3A78773671
SHA-256:	CC9690DCDE0DFA23D657F84BC221296C45590B595D5CCA9131087638C35C8A8B
SHA-512:	9720EECE674DB4F0951AD212216FFBEB779097A51152587954547B5A43BEA909ADFC7F5DFDCF55E71A622E58D85329EFBB7FBAAA80E167D102DB971F31A85921
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 26%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...K.b`.....P.....D.....^.... .....@.. ..... ..@.....O.....A.....` ....H.....text...d.... ....`.rsrc....A.....B.....@..@.rel oc.....`.....@..B.....@.....H.....^...p.....'.....0.....(....(.....(.....o....*.....(.....(!.....("....(#.....($....*N..(....o.... (%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0..<.....~.....(1.....,!r...p.....(2...o3...s4.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\LGKyjAEnmfdSo.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\wDIaJji4Vv.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210404\PowerShell_transcript.216554.9U9ReEn0.20210404023626.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):	5801
Entropy (8bit):	5.420714350260224
Encrypted:	false
SSDEEP:	96:BZDuhdNcqDo1ZJgZIhdNcqDo1Z+xTJjZOhdNcqDo1ZEcZZ4Zz:a
MD5:	53ECFAD9EEFAF0D056B9B22C5CDB6B0F
SHA1:	D4F2C61C73CEB67ADB247EA921CD5BF218B28685
SHA-256:	878AAD413BCF6A9FD72338EBEF774FC4EAF0F6D9C553730AFB1F9CC797B4EBB0
SHA-512:	BFE0BC0E42141B9FD089CEDCBA2F88148EAA9783721B54D09F0BD3119DCC2ACD4150FF1E18654A902AE1BFBE8B3185911222512D7B76F9C2528E48005F4DE0F
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210404023640..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (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\LGKyjAEnmfdSo.exe..Process ID: 5528..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: 20210404023640..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\App Data\Roaming\LGKyjAEnmfdSo.exe..**********..Windows PowerShell transcript start..Start time: 20210404024355..Username: computer\user..RunAs User: DE SKTOP-716T77

C:\Users\user\Documents\20210404\PowerShell_transcript.216554.qbfO9BC_.20210404023623.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):	5733
Entropy (8bit):	5.407583532042022
Encrypted:	false
SSDEEP:	96:BZ6hdNXqDo1ZJCZ5hdNXqDo1ZZRHJjZdhdNXqDo1ZFsZZyZh:v
MD5:	5F74AC5911D8C2C21BC9A023B35EACEB
SHA1:	010002DB241B01DAA448E55198C7176FF54B3132
SHA-256:	BDF042E980D34D15FB14DA3FFD6D1BB0A63A7A2A60DE77C72F16D112F396925F
SHA-512:	DA3E639F9AD13BD9074D34DF4AB674B21FD52A25608B46A2E16162C386699F46924C27559A87B2ADBC0304855EA7F4583BFA844F22FBECED626FDFCC49CDBD2
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210404023639..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\wDIaJji4Vv.exe..Process ID: 6104..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: 20210404023640..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\wDIaJji4Vv.exe..**********..Windows PowerShell transcript start..Start time: 20210404024000..Username: computer\user..RunAs User: computer\user..Configuration

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1145
Entropy (8bit):	4.462201512373672
Encrypted:	false
SSDEEP:	24:zKLXkzPDObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0zPDQntKKH1MqJC
MD5:	46EBEB88876A00A52CC37B1F8E0D0438
SHA1:	5E5DB352F964E5F398301662FF558BD905798A65
SHA-256:	D65BD5A6CC112838AFE8FA70BF61FD13C1313BCE3EE3E76C50E454D7B581238B
SHA-512:	E713E6F304A469FB71235C598BC7E2C6F8458ABC61DAF3D1F364F66579CAFA4A7F3023E585BDA552FB400009E7805A8CA0311A50D5EDC9C2AD2D067772A071EE
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Reconfigure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo Suppress logo output... /quiet Suppress logo output and success output...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.081468136241616
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	wDIaJji4Vv.exe
File size:	663040
MD5:	6a0c22a8a8d9524ba012910571b57d38
SHA1:	b75a74ca657f4940b251c5116bcf2d3a78773671
SHA256:	cc9690dcde0dfa23d657f84bc221296c45590b595d5cca9131087638c35c8a8b
SHA512:	9720eece674db4f0951ad212216ffbeb779097a51152587954547b5a43bea909adfc7f5dfdcf55e71a622e58d85329efbb7fbaaa80e167d102db971f31a85921
SSDEEP:	12288:7XAH590sYmLTYUxkaMjOXB7jreGkclqR:y0sYmZxfMKXBXreGk8

General

File Content Preview:	MZ......................@..!..L.!Th is program cannot be run in DOS mode....$.......PE..L... K.b`..............P......D......^.... ....@.. ....@................................

File Icon

	
Icon Hash:	716969f0f0707169

Static PE Info

General

Entrypoint:	0x49f65e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6062EC4B [Tue Mar 30 09:15:55 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9f60c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa0000	0x41fc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x9d664	0x9d800	False	0.668892609127	data	7.08932149094	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa0000	0x41fc	0x4200	False	0.279947916667	data	3.95081352234	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa6000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa0140	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 16777215, next used block 16777215		
RT_ICON	0xa26f8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xa37b0	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xa3c28	0x30	data		
RT_VERSION	0xa3c68	0x392	data		
RT_MANIFEST	0xa400c	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	Cut Rite
Assembly Version	5.1.7.18
InternalName	SparseArray.exe
FileVersion	5.1.7.18
CompanyName	Cut Rite
LegalTrademarks	

Description	Data
Comments	2000 Vector RD 180
ProductName	NamespaceResolveEventArgs
ProductVersion	5.1.7.18
FileDescription	NamespaceResolveEventArgs
OriginalFilename	SparseArray.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/04/21-02:36:28.240119	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50141	37.235.1.174	192.168.2.3
04/04/21-02:36:28.615607	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49715	6060	192.168.2.3	79.134.225.7
04/04/21-02:36:35.239306	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	6060	192.168.2.3	79.134.225.7
04/04/21-02:36:42.976818	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49722	6060	192.168.2.3	79.134.225.7
04/04/21-02:36:49.082114	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49725	6060	192.168.2.3	79.134.225.7
04/04/21-02:36:58.478341	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49729	6060	192.168.2.3	79.134.225.7
04/04/21-02:37:08.086676	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49730	6060	192.168.2.3	79.134.225.7
04/04/21-02:37:14.628009	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49732	6060	192.168.2.3	79.134.225.7
04/04/21-02:37:21.276478	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49734	6060	192.168.2.3	79.134.225.7
04/04/21-02:37:27.574430	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	6060	192.168.2.3	79.134.225.7
04/04/21-02:37:33.546247	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56338	37.235.1.174	192.168.2.3
04/04/21-02:37:33.680119	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	6060	192.168.2.3	79.134.225.7
04/04/21-02:37:42.949624	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	6060	192.168.2.3	79.134.225.7
04/04/21-02:37:49.167247	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49754	6060	192.168.2.3	79.134.225.7
04/04/21-02:37:55.222764	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49755	6060	192.168.2.3	79.134.225.7
04/04/21-02:38:01.360450	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	6060	192.168.2.3	79.134.225.7
04/04/21-02:38:07.873436	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49759	6060	192.168.2.3	79.134.225.7
04/04/21-02:38:13.888710	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49760	6060	192.168.2.3	79.134.225.7
04/04/21-02:38:21.025820	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	6060	192.168.2.3	79.134.225.7
04/04/21-02:38:27.399218	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	6060	192.168.2.3	79.134.225.7

Network Port Distribution

Total Packets: 72

- 53 (DNS)
- 6060 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 4, 2021 02:36:28.250718117 CEST	49715	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:28.389156103 CEST	6060	49715	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:28.389691114 CEST	49715	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:28.615607023 CEST	49715	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:28.767524958 CEST	6060	49715	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:28.798460960 CEST	49715	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:29.217684984 CEST	49715	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:29.351725101 CEST	6060	49715	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:29.776899099 CEST	49715	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:29.910693884 CEST	6060	49715	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:29.911135912 CEST	6060	49715	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:29.911211014 CEST	49715	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:30.105885983 CEST	49715	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:30.249970913 CEST	6060	49715	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:30.250163078 CEST	49715	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:30.438975096 CEST	6060	49715	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:30.439116955 CEST	49715	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:30.439306974 CEST	6060	49715	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:30.439351082 CEST	49715	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:30.497457981 CEST	49715	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:30.573860884 CEST	6060	49715	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:30.574028015 CEST	49715	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:30.574390888 CEST	6060	49715	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:30.575237989 CEST	49715	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:30.575354099 CEST	6060	49715	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:30.575402021 CEST	49715	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:30.575665951 CEST	6060	49715	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:30.575723886 CEST	49715	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:35.071536064 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:35.207611084 CEST	6060	49721	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:35.211637974 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:35.239305973 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:35.391490936 CEST	6060	49721	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:35.392396927 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:35.814507008 CEST	6060	49721	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:35.814668894 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:35.884809971 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:36.019741058 CEST	6060	49721	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:36.402940035 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:37.293689013 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:37.424892902 CEST	6060	49721	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:37.425476074 CEST	6060	49721	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:37.441322088 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:37.635685921 CEST	6060	49721	79.134.225.7	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 4, 2021 02:36:37.637685061 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:37.774050951 CEST	6060	49721	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:37.774080038 CEST	6060	49721	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:37.774139881 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:37.774168015 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:37.907398939 CEST	6060	49721	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:37.907434940 CEST	6060	49721	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:37.907515049 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:37.907562971 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:37.909529924 CEST	6060	49721	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:37.909603119 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:37.997713089 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:38.041229010 CEST	6060	49721	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:38.041361094 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:38.041763067 CEST	6060	49721	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:38.041857004 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:38.042584896 CEST	6060	49721	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:38.042658091 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:38.043587923 CEST	6060	49721	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:38.043687105 CEST	49721	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:42.831279039 CEST	49722	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:42.965339899 CEST	6060	49722	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:42.965501070 CEST	49722	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:42.976818085 CEST	49722	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:43.145267010 CEST	6060	49722	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:43.145742893 CEST	49722	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:43.480211020 CEST	6060	49722	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:43.481848955 CEST	49722	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:43.619811058 CEST	6060	49722	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:43.620085955 CEST	49722	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:43.956262112 CEST	6060	49722	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:43.957698107 CEST	49722	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:44.146167040 CEST	6060	49722	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:44.146250963 CEST	49722	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:44.146472931 CEST	6060	49722	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:44.146657944 CEST	49722	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:44.284683943 CEST	6060	49722	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:44.286659002 CEST	49722	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:44.287656069 CEST	6060	49722	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:44.287710905 CEST	49722	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:44.289979935 CEST	6060	49722	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:44.290055990 CEST	49722	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:44.290813923 CEST	6060	49722	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:44.292443037 CEST	49722	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:44.422521114 CEST	6060	49722	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:44.422593117 CEST	49722	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:44.422791958 CEST	6060	49722	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:44.423172951 CEST	49722	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:44.424403906 CEST	6060	49722	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:44.424593925 CEST	6060	49722	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:44.424648046 CEST	49722	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:44.428724051 CEST	6060	49722	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:44.428741932 CEST	6060	49722	79.134.225.7	192.168.2.3
Apr 4, 2021 02:36:44.428786039 CEST	49722	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:44.428814888 CEST	49722	6060	192.168.2.3	79.134.225.7
Apr 4, 2021 02:36:44.429147959 CEST	6060	49722	79.134.225.7	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 4, 2021 02:36:28.174801111 CEST	50141	53	192.168.2.3	37.235.1.174
Apr 4, 2021 02:36:28.240118980 CEST	53	50141	37.235.1.174	192.168.2.3
Apr 4, 2021 02:36:35.005397081 CEST	58823	53	192.168.2.3	37.235.1.174
Apr 4, 2021 02:36:35.055999041 CEST	53	58823	37.235.1.174	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 4, 2021 02:36:42.779943943 CEST	57568	53	192.168.2.3	37.235.1.174
Apr 4, 2021 02:36:42.829664946 CEST	53	57568	37.235.1.174	192.168.2.3
Apr 4, 2021 02:36:48.892271042 CEST	50540	53	192.168.2.3	37.235.1.174
Apr 4, 2021 02:36:48.944578886 CEST	53	50540	37.235.1.174	192.168.2.3
Apr 4, 2021 02:36:54.995816946 CEST	57762	53	192.168.2.3	37.235.1.174
Apr 4, 2021 02:36:55.047101974 CEST	53	57762	37.235.1.174	192.168.2.3
Apr 4, 2021 02:37:04.748682976 CEST	55435	53	192.168.2.3	37.235.1.174
Apr 4, 2021 02:37:04.802318096 CEST	53	55435	37.235.1.174	192.168.2.3
Apr 4, 2021 02:37:14.375236988 CEST	56132	53	192.168.2.3	37.235.1.174
Apr 4, 2021 02:37:14.425951958 CEST	53	56132	37.235.1.174	192.168.2.3
Apr 4, 2021 02:37:21.003932953 CEST	56579	53	192.168.2.3	37.235.1.174
Apr 4, 2021 02:37:21.056860924 CEST	53	56579	37.235.1.174	192.168.2.3
Apr 4, 2021 02:37:27.389853001 CEST	60633	53	192.168.2.3	37.235.1.174
Apr 4, 2021 02:37:27.440813065 CEST	53	60633	37.235.1.174	192.168.2.3
Apr 4, 2021 02:37:33.479202032 CEST	56338	53	192.168.2.3	37.235.1.174
Apr 4, 2021 02:37:33.546247005 CEST	53	56338	37.235.1.174	192.168.2.3
Apr 4, 2021 02:37:39.720015049 CEST	56803	53	192.168.2.3	37.235.1.174
Apr 4, 2021 02:37:39.799464941 CEST	53	56803	37.235.1.174	192.168.2.3
Apr 4, 2021 02:37:48.864392996 CEST	57145	53	192.168.2.3	37.235.1.174
Apr 4, 2021 02:37:48.921525002 CEST	53	57145	37.235.1.174	192.168.2.3
Apr 4, 2021 02:37:55.037035942 CEST	55359	53	192.168.2.3	37.235.1.174
Apr 4, 2021 02:37:55.087060928 CEST	53	55359	37.235.1.174	192.168.2.3
Apr 4, 2021 02:38:01.165364027 CEST	58306	53	192.168.2.3	37.235.1.174
Apr 4, 2021 02:38:01.216670990 CEST	53	58306	37.235.1.174	192.168.2.3
Apr 4, 2021 02:38:07.390798092 CEST	63150	53	192.168.2.3	37.235.1.174
Apr 4, 2021 02:38:07.577543020 CEST	53	63150	37.235.1.174	192.168.2.3
Apr 4, 2021 02:38:13.693104029 CEST	53279	53	192.168.2.3	37.235.1.174
Apr 4, 2021 02:38:13.753438950 CEST	53	53279	37.235.1.174	192.168.2.3
Apr 4, 2021 02:38:20.840424061 CEST	56881	53	192.168.2.3	37.235.1.174
Apr 4, 2021 02:38:20.892973900 CEST	53	56881	37.235.1.174	192.168.2.3
Apr 4, 2021 02:38:27.215109110 CEST	53642	53	192.168.2.3	37.235.1.174
Apr 4, 2021 02:38:27.264962912 CEST	53	53642	37.235.1.174	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 4, 2021 02:36:28.174801111 CEST	192.168.2.3	37.235.1.174	0xcd1f	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Apr 4, 2021 02:36:35.005397081 CEST	192.168.2.3	37.235.1.174	0x7824	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Apr 4, 2021 02:36:42.779943943 CEST	192.168.2.3	37.235.1.174	0x8e5e	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Apr 4, 2021 02:36:48.892271042 CEST	192.168.2.3	37.235.1.174	0xc05	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Apr 4, 2021 02:36:54.995816946 CEST	192.168.2.3	37.235.1.174	0xc323	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Apr 4, 2021 02:37:04.748682976 CEST	192.168.2.3	37.235.1.174	0xb23e	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Apr 4, 2021 02:37:14.375236988 CEST	192.168.2.3	37.235.1.174	0x7aa1	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Apr 4, 2021 02:37:21.003932953 CEST	192.168.2.3	37.235.1.174	0x8b21	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Apr 4, 2021 02:37:27.389853001 CEST	192.168.2.3	37.235.1.174	0xae49	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Apr 4, 2021 02:37:33.479202032 CEST	192.168.2.3	37.235.1.174	0x42f5	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Apr 4, 2021 02:37:39.720015049 CEST	192.168.2.3	37.235.1.174	0x8dec	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Apr 4, 2021 02:37:48.864392996 CEST	192.168.2.3	37.235.1.174	0x2055	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Apr 4, 2021 02:37:55.037035942 CEST	192.168.2.3	37.235.1.174	0xe1c3	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Apr 4, 2021 02:38:01.165364027 CEST	192.168.2.3	37.235.1.174	0x3943	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Apr 4, 2021 02:38:07.390798092 CEST	192.168.2.3	37.235.1.174	0x7532	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Apr 4, 2021 02:38:13.693104029 CEST	192.168.2.3	37.235.1.174	0x7aac	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 4, 2021 02:38:20.840424061 CEST	192.168.2.3	37.235.1.174	0x7b82	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Apr 4, 2021 02:38:27.215109110 CEST	192.168.2.3	37.235.1.174	0xfd2a	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)

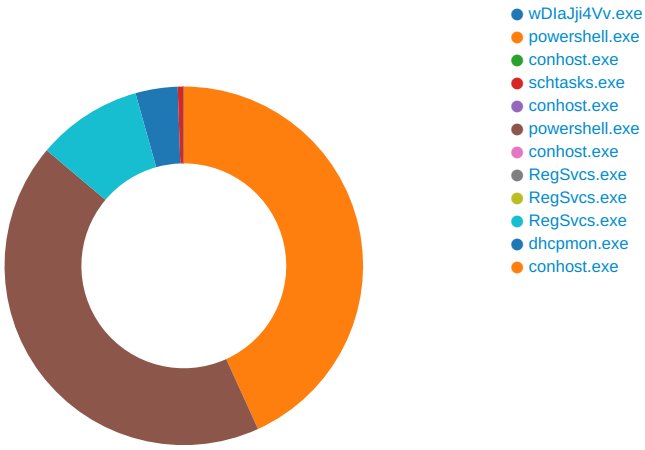
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 4, 2021 02:36:28.240118980 CEST	37.235.1.174	192.168.2.3	0xcd1f	No error (0)	james12.ddns.net		79.134.225.7	A (IP address)	IN (0x0001)
Apr 4, 2021 02:36:35.055999041 CEST	37.235.1.174	192.168.2.3	0x7824	No error (0)	james12.ddns.net		79.134.225.7	A (IP address)	IN (0x0001)
Apr 4, 2021 02:36:42.829664946 CEST	37.235.1.174	192.168.2.3	0x8e5e	No error (0)	james12.ddns.net		79.134.225.7	A (IP address)	IN (0x0001)
Apr 4, 2021 02:36:48.944578886 CEST	37.235.1.174	192.168.2.3	0xc05	No error (0)	james12.ddns.net		79.134.225.7	A (IP address)	IN (0x0001)
Apr 4, 2021 02:36:55.047101974 CEST	37.235.1.174	192.168.2.3	0xc323	No error (0)	james12.ddns.net		79.134.225.7	A (IP address)	IN (0x0001)
Apr 4, 2021 02:37:04.802318096 CEST	37.235.1.174	192.168.2.3	0xb23e	No error (0)	james12.ddns.net		79.134.225.7	A (IP address)	IN (0x0001)
Apr 4, 2021 02:37:14.425951958 CEST	37.235.1.174	192.168.2.3	0x7aa1	No error (0)	james12.ddns.net		79.134.225.7	A (IP address)	IN (0x0001)
Apr 4, 2021 02:37:21.056860924 CEST	37.235.1.174	192.168.2.3	0x8b21	No error (0)	james12.ddns.net		79.134.225.7	A (IP address)	IN (0x0001)
Apr 4, 2021 02:37:27.440813065 CEST	37.235.1.174	192.168.2.3	0xae49	No error (0)	james12.ddns.net		79.134.225.7	A (IP address)	IN (0x0001)
Apr 4, 2021 02:37:33.546247005 CEST	37.235.1.174	192.168.2.3	0x42f5	No error (0)	james12.ddns.net		79.134.225.7	A (IP address)	IN (0x0001)
Apr 4, 2021 02:37:39.799464941 CEST	37.235.1.174	192.168.2.3	0x8dec	No error (0)	james12.ddns.net		79.134.225.7	A (IP address)	IN (0x0001)
Apr 4, 2021 02:37:48.921525002 CEST	37.235.1.174	192.168.2.3	0x2055	No error (0)	james12.ddns.net		79.134.225.7	A (IP address)	IN (0x0001)
Apr 4, 2021 02:37:55.087060928 CEST	37.235.1.174	192.168.2.3	0xe1c3	No error (0)	james12.ddns.net		79.134.225.7	A (IP address)	IN (0x0001)
Apr 4, 2021 02:38:01.216670990 CEST	37.235.1.174	192.168.2.3	0x3943	No error (0)	james12.ddns.net		79.134.225.7	A (IP address)	IN (0x0001)
Apr 4, 2021 02:38:07.577543020 CEST	37.235.1.174	192.168.2.3	0x7532	No error (0)	james12.ddns.net		79.134.225.7	A (IP address)	IN (0x0001)
Apr 4, 2021 02:38:13.753438950 CEST	37.235.1.174	192.168.2.3	0x7aac	No error (0)	james12.ddns.net		79.134.225.7	A (IP address)	IN (0x0001)
Apr 4, 2021 02:38:20.892973900 CEST	37.235.1.174	192.168.2.3	0x7b82	No error (0)	james12.ddns.net		79.134.225.7	A (IP address)	IN (0x0001)
Apr 4, 2021 02:38:27.264962912 CEST	37.235.1.174	192.168.2.3	0xfd2a	No error (0)	james12.ddns.net		79.134.225.7	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: wDlaJji4Vv.exe PID: 2788 Parent PID: 5636

General

Start time:	02:36:19
Start date:	04/04/2021
Path:	C:\Users\user\Desktop\wDlaJji4Vv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\wDlaJji4Vv.exe'
Imagebase:	0x9a0000
File size:	663040 bytes
MD5 hash:	6A0C22A8A8D9524BA012910571B57D38
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.221605771.0000000004202000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.221605771.0000000004202000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.221605771.0000000004202000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.217455924.0000000003191000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	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	72FB60AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\LGKyjAEnmfdSo.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	588047C	CopyFileW
C:\Users\user\AppData\Roaming\LGKyjAEnmfdSo.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	588047C	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpE049.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5880A40	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\wDIaJji4Vv.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE049.tmp	success or wait	1	5880EB6	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\LGKyjAEnmfdSo.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 4b ec 62 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 d8 09 00 00 44 00 00 00 00 00 00 5e f6 09 00 00 20 00 00 00 00 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 80 0a 00 00 02 00 00 00 00 00 00 02 00 40 85 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.... $.......PE..L...K.b`.......... ....P......D......^.... ....@.. ....@................	success or wait	3	588047C	CopyFileW
C:\Users\user\AppData\Roaming\LGKyjAEnmfdSo.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	588047C	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE049.tmp	unknown	1646	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 3e 0d 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 0d 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 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?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>.. </RegistrationIn	success or wait	1	5880CCF	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\wDIaJji4Vv.exe.log	unknown	664	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: powershell.exe PID: 6104 Parent PID: 2788

General

Start time:	02:36:21
Start date:	04/04/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\wDIaJji4Vv.exe'
Imagebase:	0xb00000
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	6D81CF06	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	6D81CF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C5C5B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C5C5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wlk4xu4b.yrc.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C661E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bn2wvdhj.h2i.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C661E60	CreateFileW
C:\Users\user\Documents\20210404	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C66BEFF	CreateDirectoryW
C:\Users\user\Documents\20210404\PowerShell_transcript.216554.qbfO9BC_.20210404023623.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C661E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C661E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wlk4xu4b.yrc.ps1	success or wait	1	6C666A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bn2wvdhj.h2i.psm1	success or wait	1	6C666A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wlk4xu4b.yrc.ps1	unknown	1	31	1	success or wait	1	6C661B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bn2wvdhj.h2i.psm1	unknown	1	31	1	success or wait	1	6C661B4F	WriteFile
C:\Users\user\Documents\20210404\PowerShell_transcript.216554.qbfO9BC_.20210404023623.txt	unknown	3	ef bb bf	...	success or wait	1	6C661B4F	WriteFile
C:\Users\user\Documents\20210404\PowerShell_transcript.216554.qbfO9BC_.20210404023623.txt	unknown	669	2a 2a 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 31 30 34 30 34 30 32 33 36 33 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 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 32 31 36 35 35 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20210404023639..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	44	6C661B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....<.e....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6C661B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.....Remove-Variable.....Convert-String.....Trace-Command.....Sort-Object.....Register-ObjectEvent.....Get-Runspace.....Format-Table.....Wait-Debugger.....Get-Runspac	success or wait	1	6C661B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 ce 12 09 ca 9f d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	6C661B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2446	10 00 00 00 52 65 73 75 6d 65 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 1c 00 00 00 42 61 63 6b 75 70 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 25 00 00 00 53 68 6f 77 2d 42 69 74 4c 6f 63 6b 65 72 52 65 71 75 69 72 65 64 41 63 74 69 6f 6e 73 49 6e 74 65 72 6e 61 6c 02 00 00 00 17 00 00 00 55 6e 6c 6f 63 6b 2d 50 61 73 73 77 6f 72 64 49 6e 74 65 72 6e 61 6c 02 00 00 00 10 00 00 00 55 6e 6c 6f 63 6b 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 18 00 00 00 41 64 64 2d 54 70 6d 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 25 00 00 00 41 64 64 2d 52 65 63 6f 76 65 72 79 50 61 73 73 77 6f 72 64 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 55 6e 6c 6f 63 6b 2d 52 65 63 6f 76 65 72	....Resume-BitLocker.....Backup-BitLockerKeyProtector....%...Show-BitLockerRequiredActionsInternal.....Unlock-PasswordInternal.....Unlock-BitLocker.....Add-TpmProtectorInternal....%...Add-RecoveryPasswordProtectorInternal.....Unlock-Recover	success or wait	1	6C661B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 65 14 00 00 18 00 00 00 ea 0d 0d 05 dd 08 cb 08 ab 08 00 00 00 00 69 02 39 00 ca 0d 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....e.....i.9.....@.....	success or wait	1	6DAE76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 3c 00 00 00 0e 00 20 00	H.....<@.^...L."My...:<..... .	success or wait	17	6DAE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	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	6DAE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6DAE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6DAE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 54 01 40 00 ce 67 40 01 f9 3e 40 01 99 01 40 00 fb 00 40 00 cb 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 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 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 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 00 01 7a 54 00 01 95 54 00 01 3d 4d 00 01 44 4d 00 01 3a 4d 00 01 22 4d 00 01 20 4d 00 01 21 4d 00 01 3b 4d 00 01 e0 44 00 01 e5 44 00 01 40 4d 00 01 3c 4d 00 01 24 4d 00 01 38 4d 00 01 3f 4d 00 01 16 3b 40 01 42 4d 00 01 ed 44 00 01 6d 45 00 01 45 4d 00 01 dc 71 00 01 dd 71 00 01 f8 53 00 01 98 25 00	.....T.@..g@..>@...@...@...@.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...%.	success or wait	11	6DAE76FC	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	6D7F5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7FCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7FCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7F5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7F5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7F5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D7503DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7F5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D801F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21312	success or wait	1	6D80203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7503DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	129	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D7503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7F5705	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	6D7F5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7F5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7F5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	71	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C661B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C661B4F	ReadFile

Analysis Process: conhost.exe PID: 404 Parent PID: 6104

General

Start time:	02:36:21
Start date:	04/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 3120 Parent PID: 2788

General

Start time:	02:36:21
Start date:	04/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\LGKyjAEnmfdSo' /XML 'C:\Users\user\AppData\Local\Temp\tmpE049.tmp'
Imagebase:	0x360000
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\tmpE049.tmp	unknown	2	success or wait	1	36AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE049.tmp	unknown	1647	success or wait	1	36ABD9	ReadFile

Analysis Process: conhost.exe PID: 6100 Parent PID: 3120

General

Start time:	02:36:22
Start date:	04/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 5528 Parent PID: 2788

General

Start time:	02:36:22
Start date:	04/04/2021
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\LGKyjAEnmfdSo.exe'
Imagebase:	0xb00000
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	6D81CF06	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	6D81CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jbmpopxb.30w.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C661E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_z5wqclte.tm2.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C661E60	CreateFileW
C:\Users\user\Documents\20210404\PowerShell_transcript.216554.9U9ReEn0.20210404023626.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C661E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jbmpopxb.30w.ps1	success or wait	1	6C666A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_z5wqclte.tm2.psm1	success or wait	1	6C666A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jbmpopxb.30w.ps1	unknown	1	31	1	success or wait	1	6C661B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_z5wqclte.tm2.psm1	unknown	1	31	1	success or wait	1	6C661B4F	WriteFile
C:\Users\user\Documents\20210404\PowerShell_transcript.216554.9U9ReEn0.20210404023626.txt	unknown	3	ef bb bf	...	success or wait	1	6C661B4F	WriteFile
C:\Users\user\Documents\20210404\PowerShell_transcript.216554.9U9ReEn0.20210404023626.txt	unknown	680	2a 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 31 30 34 30 34 30 32 33 36 34 30 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 32 31 36 35 35 34 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********..Windows PowerShell transcript start..Start time: 20210404023640..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	44	6C661B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....<.e....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6C661B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.....Remove-Variable.....Convert-String.....Trace-Command.....Sort-Object.....Register-ObjectEvent.....Get-Runspace.....Format-Table.....Wait-Debugger.....Get-Runspac	success or wait	1	6C661B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 ce 12 09 ca 9f d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	6C661B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2446	10 00 00 00 52 65 73 75 6d 65 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 1c 00 00 00 42 61 63 6b 75 70 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 25 00 00 00 53 68 6f 77 2d 42 69 74 4c 6f 63 6b 65 72 52 65 71 75 69 72 65 64 41 63 74 69 6f 6e 73 49 6e 74 65 72 6e 61 6c 02 00 00 00 17 00 00 00 55 6e 6c 6f 63 6b 2d 50 61 73 73 77 6f 72 64 49 6e 74 65 72 6e 61 6c 02 00 00 00 10 00 00 00 55 6e 6c 6f 63 6b 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 18 00 00 00 41 64 64 2d 54 70 6d 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 25 00 00 00 41 64 64 2d 52 65 63 6f 76 65 72 79 50 61 73 73 77 6f 72 64 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 55 6e 6c 6f 63 6b 2d 52 65 63 6f 76 65 72	....Resume-BitLocker.....Backup-BitLockerKeyProtector....%...Show-BitLockerRequiredActionsInternal.....Unlock-PasswordInternal.....Unlock-BitLocker.....Add-TpmProtectorInternal....%...Add-RecoveryPasswordProtectorInternal.....Unlock-Recover	success or wait	1	6C661B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 80 14 00 00 18 00 00 00 ea 0d 16 05 d4 08 c0 08 a0 08 00 00 00 00 3c 02 34 00 ca 0d 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....<.4.....@.....	success or wait	1	6DAE76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	44 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 66 5a 76 65 a7 f4 b9 46 9f a9 b0 89 11 78 b4 29 f9 12 00 00 0e 00 1c 00	D.....fZve...F.....x .).....	success or wait	17	6DAE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	28	53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e	System.Management.Automation	success or wait	17	6DAE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6DAE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6DAE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	01 0e 80 00 00 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 be 3c 40 00 57 03 40 00 4d 03 40 00 f0 45 40 00 54 01 40 01 f9 3e 40 00 cb 00 40 01 56 01 40 01 48 01 40 01 58 01 40 01 5b 01 40 01 4e 54 40 00 48 54 40 00 f4 53 40 00 8b 53 40 00 68 54 40 00 91 53 40 00 fa 53 40 00 82 53 40 00 5c 01 40 01 00 54 40 00 02 54 40 00 40 58 40 00 3f 58 40 00 1c 54 40 00 b8 53 40 00 fb 53 40 00 1e 54 40 00 19 54 40 00 78 54 40 00 7a 54 40 00 95 54 40 00 3d 4d 40 00 44 4d 40 00 3a 4d 40 00 22 4d 40 00 20 4d 40 00 21 4d 40 00 3b 4d 40 00 e0 44 40 00 e5 44 40 00 40 4d 40 00 3c 4d 40 00 24 4d 40 00 38 4d 40 00 3f 4d 40 00 42 4d 00 00 ed 44 00 00 6d 45 00 00 45 4d 00 00 dc 71 00 00 dd 71 00 00 f8 53 00 00 98 25 00	.....<@.W.@.M.@..E@.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...%.	success or wait	11	6DAE76FC	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	6D7F5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7FCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7FCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7F5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7F5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7F5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D7503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7F5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7F5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D801F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21312	success or wait	1	6D80203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7503DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation \1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	137	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C661B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D7503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7F5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7F5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D7F5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D7F5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6C661B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C661B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C661B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C661B4F	ReadFile

Analysis Process: conhost.exe PID: 4812 Parent PID: 5528

General

Start time:	02:36:23
Start date:	04/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: RegSvcs.exe PID: 4688 Parent PID: 2788

General

Start time:	02:36:23
Start date:	04/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0x1b0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegSvcs.exe PID: 6172 Parent PID: 2788

General

Start time:	02:36:23
Start date:	04/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0x320000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegSvcs.exe PID: 6228 Parent PID: 2788

General

Start time:	02:36:24
Start date:	04/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0xfb0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.484889407.0000000006880000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.484889407.0000000006880000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.484797009.0000000006840000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.484797009.0000000006840000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.485602336.0000000006D40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.485602336.0000000006D40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 0000000C.00000003.451562866.0000000004A08000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.484953222.00000000068B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.484953222.00000000068B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.480310164.0000000003664000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.484912246.0000000006890000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.484912246.0000000006890000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.484650289.00000000067B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.484650289.00000000067B0000.00000004.00000001.sdmp, Author: Florian Roth

	• Rule: NanoCore, Description: unknown, Source: 0000000C.00000003.462233359.0000000004945000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.484681647.00000000067C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.484681647.00000000067C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.482083953.000000000466E000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.484707713.00000000067E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.484707713.00000000067E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.484868495.0000000006870000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.484868495.0000000006870000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.467839599.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.467839599.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.467839599.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.484846998.0000000006860000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.484846998.0000000006860000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.485000098.00000000068D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.485000098.00000000068D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.485021734.00000000068E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.485021734.00000000068E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.484030724.0000000005C20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.484030724.0000000005C20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.484199869.0000000005EC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.484199869.0000000005EC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.484199869.0000000005EC0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

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	72FB60AC	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	72FB60AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	58A07A1	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	58A089B	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	58A07A1	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	58A0B20	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	58A07A1	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	58A07A1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	15	58A089B	CreateFileW

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	unknown	8	e1 d5 e3 1d 4d f7 d8 48	....M..H	success or wait	1	58A0A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	32768	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 cf ce 7b 5a 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 08 00 00 50 00 00 00 20 00 00 00 00 00 00 de 6b 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 00 00 00 10 00 00 b1 5b 01 00 03 00 40 05 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....$.......PE..L..... {Z.................P... ....k... ....@.. ....[....@................	success or wait	1	58A0B20	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b........4h...t .+..Z\.. .i.......@.3..{...grv +V.....B.......].P...W.4C}uL.. ...s~..F...}.......E......E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	10	58A0A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	58A0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	success or wait	1	58A0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	end of file	1	58A0A53	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7308BF06	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	58A0C12	RegSetValueExW

Analysis Process: dhcpmon.exe PID: 6744 Parent PID: 3388

General

Start time:	02:36:39
Start date:	04/04/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x6f0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

Analysis Process: conhost.exe PID: 6752 Parent PID: 6744

General

Start time:	02:36:39
Start date:	04/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis