

JOeSandbox Cloud BASIC



ID: 411514

Sample Name:

y3t4g48gj6_PAYMENT.exe

Cookbook: default.jbs

Time: 23:52:33

Date: 11/05/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report y3t4g48gj6_PAYMENT.exe	5
Overview	5
General Information	5
Detection	5
Signatures	5
Classification	5
Startup	5
Malware Configuration	5
Threatname: NanoCore	5
Yara Overview	6
Memory Dumps	6
Unpacked PEs	6
Sigma Overview	7
AV Detection:	7
E-Banking Fraud:	7
System Summary:	7
Stealing of Sensitive Information:	7
Remote Access Functionality:	7
Signature Overview	7
AV Detection:	8
Networking:	8
E-Banking Fraud:	8
System Summary:	8
Persistence and Installation Behavior:	8
Boot Survival:	8
Hooking and other Techniques for Hiding and Protection:	8
Malware Analysis System Evasion:	8
Anti Debugging:	9
HIPS / PFW / Operating System Protection Evasion:	9
Stealing of Sensitive Information:	9
Remote Access Functionality:	9
Mitre Att&ck Matrix	9
Behavior Graph	9
Screenshots	10
Thumbnails	10
Antivirus, Machine Learning and Genetic Malware Detection	11
Initial Sample	11
Dropped Files	11
Unpacked PE Files	11
Domains	11
URLs	11
Domains and IPs	12
Contacted Domains	12
Contacted URLs	12
URLs from Memory and Binaries	12
Contacted IPs	13
Public	14
Private	14
General Information	14
Simulations	16
Behavior and APIs	16
Joe Sandbox View / Context	16
IPs	16
Domains	16
ASN	16

JA3 Fingerprints	16
Dropped Files	17
Created / dropped Files	17
Static File Info	24
General	24
File Icon	24
Static PE Info	24
General	24
Authenticode Signature	25
Entrypoint Preview	25
Data Directories	26
Sections	27
Resources	27
Imports	27
Version Infos	27
Network Behavior	27
Network Port Distribution	27
TCP Packets	28
UDP Packets	29
DNS Queries	31
DNS Answers	31
Code Manipulations	31
Statistics	31
Behavior	31
System Behavior	32
Analysis Process: y3t4g48gj6_PAYMENT.exe PID: 7028 Parent PID: 5908	32
General	32
File Activities	32
File Created	32
File Written	33
File Read	33
Registry Activities	34
Key Created	34
Key Value Created	34
Analysis Process: svchost.exe PID: 7128 Parent PID: 560	34
General	34
File Activities	34
Analysis Process: powershell.exe PID: 4668 Parent PID: 7028	35
General	35
File Activities	35
File Created	35
File Deleted	35
File Written	36
File Read	38
Analysis Process: conhost.exe PID: 4104 Parent PID: 4668	41
General	41
Analysis Process: powershell.exe PID: 4896 Parent PID: 7028	41
General	41
File Activities	42
File Created	42
File Deleted	42
File Written	42
File Read	45
Analysis Process: conhost.exe PID: 4524 Parent PID: 4896	48
General	48
Analysis Process: powershell.exe PID: 1912 Parent PID: 7028	48
General	48
File Activities	48
File Created	48
File Deleted	49
File Written	49
File Read	52
Analysis Process: conhost.exe PID: 6408 Parent PID: 1912	55
General	55
Analysis Process: cmd.exe PID: 6336 Parent PID: 7028	55
General	55
Analysis Process: conhost.exe PID: 6356 Parent PID: 6336	55
General	55
Analysis Process: timeout.exe PID: 4752 Parent PID: 6336	55
General	56

Analysis Process: y3t4g48gj6_PAYMENT.exe PID: 6644 Parent PID: 7028	56
General	56
Analysis Process: y3t4g48gj6_PAYMENT.exe PID: 6868 Parent PID: 7028	56
General	56
Analysis Process: svchost.exe PID: 7088 Parent PID: 560	56
General	56
Analysis Process: svchost.exe PID: 6824 Parent PID: 3440	57
General	57
Analysis Process: svchost.exe PID: 4696 Parent PID: 560	57
General	57
Analysis Process: WerFault.exe PID: 6396 Parent PID: 4696	57
General	57
Analysis Process: WerFault.exe PID: 5760 Parent PID: 7028	58
General	58
Analysis Process: svchost.exe PID: 5980 Parent PID: 3440	58
General	58
Analysis Process: svchost.exe PID: 6160 Parent PID: 560	58
General	58
Analysis Process: svchost.exe PID: 5280 Parent PID: 560	58
General	58
Analysis Process: svchost.exe PID: 2032 Parent PID: 560	59
General	59
Disassembly	59
Code Analysis	59

Analysis Report y3t4g48gj6_PAYMENT.exe

Overview

General Information

Sample Name:	y3t4g48gj6_PAYMENT.exe
Analysis ID:	411514
MD5:	9998f7e0c708ba1.
SHA1:	e3810d21600bb0..
SHA256:	9f44f33f1b0b724...
Infos:	
Most interesting Screenshot:	

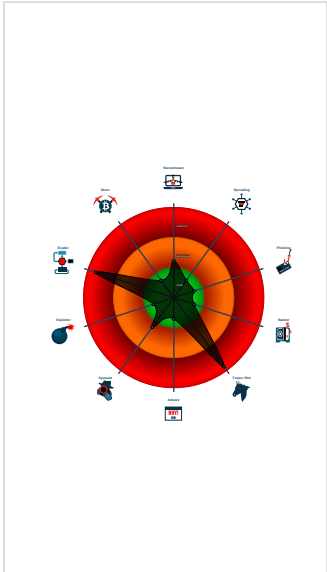
Detection

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
Yara detected Nanocore RAT
Adds a directory exclusion to Windo...
C2 URLs / IPs found in malware con...
Creates an autostart registry key po...
Drops PE files with benign system n...
Drops executables to the windows d...
Hides that the sample has been dow...
Hides threads from debuggers

Classification



Startup

- System is w10x64
- y3t4g48gj6_PAYMENT.exe (PID: 7028 cmdline: 'C:\Users\user\Desktop\y3t4g48gj6_PAYMENT.exe' MD5: 9998F7E0C708BA1FA4B56235A9811C0F)
 - powershell.exe (PID: 4668 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\lagcQ435Jh2M0514\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
 - conhost.exe (PID: 4104 cmdline: 'C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - powershell.exe (PID: 4896 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\y3t4g48gj6_PAYMENT.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
 - conhost.exe (PID: 4524 cmdline: 'C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - powershell.exe (PID: 1912 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\lagcQ435Jh2M0514\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
 - conhost.exe (PID: 6408 cmdline: 'C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - cmd.exe (PID: 6336 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
 - conhost.exe (PID: 6356 cmdline: 'C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - timeout.exe (PID: 4752 cmdline: timeout 1 MD5: 121A4EDA60A7AF65DFA82F7BB95659)
 - y3t4g48gj6_PAYMENT.exe (PID: 6644 cmdline: 'C:\Users\user\Desktop\y3t4g48gj6_PAYMENT.exe' MD5: 9998F7E0C708BA1FA4B56235A9811C0F)
 - y3t4g48gj6_PAYMENT.exe (PID: 6868 cmdline: 'C:\Users\user\Desktop\y3t4g48gj6_PAYMENT.exe' MD5: 9998F7E0C708BA1FA4B56235A9811C0F)
 - WerFault.exe (PID: 5760 cmdline: 'C:\Windows\SysWOW64\WerFault.exe -u -p 7028 -s 1780 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
 - svchost.exe (PID: 7128 cmdline: 'C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
 - svchost.exe (PID: 7088 cmdline: 'C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
 - svchost.exe (PID: 6824 cmdline: 'C:\Windows\Resources\Themes\lagcQ435Jh2M0514\svchost.exe' MD5: 9998F7E0C708BA1FA4B56235A9811C0F)
 - svchost.exe (PID: 4696 cmdline: 'C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
 - WerFault.exe (PID: 6396 cmdline: 'C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 7028 -ip 7028 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
 - svchost.exe (PID: 5980 cmdline: 'C:\Windows\Resources\Themes\lagcQ435Jh2M0514\svchost.exe' MD5: 9998F7E0C708BA1FA4B56235A9811C0F)
 - svchost.exe (PID: 6160 cmdline: 'C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
 - svchost.exe (PID: 5280 cmdline: 'C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
 - svchost.exe (PID: 2032 cmdline: 'C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- cleanup

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "f8dfffc54-Sec5-4013-9de8-d8d85368",
  "Group": "CODEDBASE",
  "Domain1": "omaprilcode.duckdns.org",
  "Domain2": "omaprilcode.duckdns.org",
  "Port": 8090,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "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": "8.8.8.8"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.600696980.00000000046E 1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0x3bf37d:\$x1: NanoCore.ClientPluginHost 0x3bf3ba:\$x2: IClientNetworkHost 0x3c2eed:\$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJlLdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000001.00000002.600696980.00000000046E 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000001.00000002.600696980.00000000046E 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@technarchy.net>	0x3bf0e5:\$a: NanoCore 0x3bf0f5:\$a: NanoCore 0x3bf329:\$a: NanoCore 0x3bf33d:\$a: NanoCore 0x3bf37d:\$a: NanoCore 0x3bf144:\$b: ClientPlugin 0x3bf346:\$b: ClientPlugin 0x3bf386:\$b: ClientPlugin 0x3bf26b:\$c: ProjectData 0x3bfc72:\$d: DESCrypto 0x3c763e:\$e: KeepAlive 0x3c562c:\$g: LogClientMessage 0x3c1827:\$i: get_Connected 0x3bffa8:\$j: #=q 0x3bfd8:\$j: #=q 0x3bff4:\$j: #=q 0x3c0024:\$j: #=q 0x3c0040:\$j: #=q 0x3c005c:\$j: #=q 0x3c008c:\$j: #=q 0x3c00a8:\$j: #=q
Process Memory Space: y3t4g48gj6_PAYMENT.exe PID: 7028	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0x5ecd3:\$x1: NanoCore.ClientPluginHost 0x5ed034:\$x2: IClientNetworkHost 0x5f2439:\$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJlLdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe 0x6003ab:\$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJlLdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Process Memory Space: y3t4g48gj6_PAYMENT.exe PID: 7028	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 1 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
--------	------	-------------	--------	---------

Source	Rule	Description	Author	Strings
1.2.y3t4g48gj6_PAYMENT.exe.4a901f0.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0xe38d:\$x1: NanoCore.ClientPluginHost 0xe3ca:\$x2: IClientNetworkHost 0x11efd:\$x3: #=qjgz7Jmpp0J7FvL9dmi8ctJILDgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcfp8PZGe
1.2.y3t4g48gj6_PAYMENT.exe.4a901f0.1.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	0xe105:\$x1: NanoCore.Client.exe 0xe38d:\$x2: NanoCore.ClientPluginHost 0xf9c6:\$s1: PluginCommand 0xf9ba:\$s2: FileCommand 0x1086b:\$s3: PipeExists 0x16622:\$s4: PipeCreated 0xe3b7:\$s5: IClientLoggingHost
1.2.y3t4g48gj6_PAYMENT.exe.4a901f0.1.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
1.2.y3t4g48gj6_PAYMENT.exe.4a901f0.1.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0xe0f5:\$a: NanoCore 0xe105:\$a: NanoCore 0xe339:\$a: NanoCore 0xe34d:\$a: NanoCore 0xe38d:\$a: NanoCore 0xe154:\$b: ClientPlugin 0xe356:\$b: ClientPlugin 0xe396:\$b: ClientPlugin 0xe27b:\$c: ProjectData 0xec82:\$d: DESCrypto 0x1664e:\$e: KeepAlive 0x1463c:\$g: LogClientMessage 0x10837:\$i: get_Connected 0xefb8:\$j: #=q 0xefeb:\$j: #=q 0xf004:\$j: #=q 0xf034:\$j: #=q 0xf050:\$j: #=q 0xf06c:\$j: #=q 0xf09c:\$j: #=q 0xf0b8:\$j: #=q
1.2.y3t4g48gj6_PAYMENT.exe.4a901f0.1.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0x1018d:\$x1: NanoCore.ClientPluginHost 0x101ca:\$x2: IClientNetworkHost 0x13cfd:\$x3: #=qjgz7Jmpp0J7FvL9dmi8ctJILDgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcfp8PZGe

Click to see the 3 entries

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Non Interactive PowerShell

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

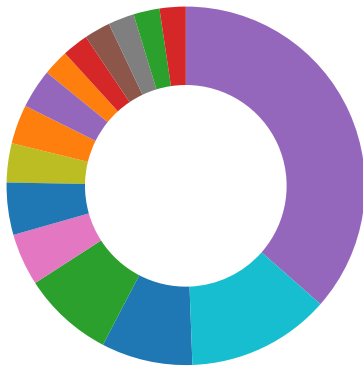
Sigma detected: NanoCore

Signature Overview

- AV Detection
- Compliance
- Networking
- E-Banking Fraud

Copyright Joe Security LLC 2021

Page 7 of 59



- 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
- 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:



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)

Initial sample is a PE file and has a suspicious name

Persistence and Installation Behavior:



Drops PE files with benign system names

Drops executables to the windows directory (C:\Windows) and starts them

Boot Survival:



Creates an autostart registry key pointing to binary in C:\Windows

Hooking and other Techniques for Hiding and Protection:



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

Malware Analysis System Evasion:



Tries to delay execution (extensive OutputDebugStringW loop)

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

Anti Debugging:



Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:



Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

Stealing of Sensitive Information:



Yara detected Nanocore RAT

Remote Access Functionality:



Detected Nanocore Rat

Yara detected Nanocore RAT

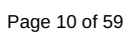
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder 1 1	Process Injection 1 1 1	Masquerading 2 2 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communications
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Disable or Modify Tools 1 1	LSASS Memory	Security Software Discovery 3 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redirected Calls/Service
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 5 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit Track C Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Virtualization/Sandbox Evasion 2 5 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manipulate Device Communications
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Timestomp 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 2 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

Behavior Graph



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
y3t4g48gj6_PAYMENT.exe	15%	ReversingLabs	Win32.Trojan.Generic	
y3t4g48gj6_PAYMENT.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Resources\Themes\agcQ435Jh2M0514\svchost.exe	100%	Joe Sandbox ML		
C:\Windows\Resources\Themes\agcQ435Jh2M0514\svchost.exe	15%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
omapiilcode.duckdns.org	3%	VirusTotal		Browse

URLs

Source	Detection	Scanner	Label	Link
omaprillcode.duckdns.org	3%	Virustotal		Browse
omaprillcode.duckdns.org	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
omaprillcode.duckdns.org	194.5.97.75	true	true	3%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
omaprillcode.duckdns.org	true	3%, Virustotal, Browse - Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirthrh http://schemas.xmlsoap.org/ws/2005	WerFault.exe, 00000014.00000000 3.444890733.0000000005230000.0 00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	WerFault.exe, 00000014.00000000 3.444890733.0000000005230000.0 00000004.00000001.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000005.00000 003.482507210.000000000812F000 .00000004.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress http://schemas.xmlsoap.org/ws/200	WerFault.exe, 00000014.00000000 3.444890733.0000000005230000.0 00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000005.00000 003.482507210.000000000812F000 .00000004.00000001.sdmp	false		high
http://https://corp.roblox.com/contact/	svchost.exe, 0000001B.00000003 .494731203.00000193D751E000.00 0000004.00000001.sdmp, svchost.exe, 0000001B.00000003.4943129 84.00000193D75AB000.00000004.0 0000001.sdmp	false		high
http://https://go.micro	powershell.exe, 00000007.00000 003.511991021.000000000552F000 .00000004.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown
http://https://www.roblox.com/develop	svchost.exe, 0000001B.00000003 .494731203.00000193D751E000.00 0000004.00000001.sdmp, svchost.exe, 0000001B.00000003.4943129 84.00000193D75AB000.00000004.0 0000001.sdmp	false		high
http://https://instagram.com/hiddency_	svchost.exe, 0000001B.00000003 .462561929.00000193D7577000.00 0000004.00000001.sdmp, svchost.exe, 0000001B.00000003.4632077 61.00000193D758D000.00000004.0 0000001.sdmp, svchost.exe, 000 0001B.00000003.462293843.00000 193D756D000.00000004.00000001. sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone	WerFault.exe, 00000014.00000000 3.444890733.0000000005230000.0 00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone	WerFault.exe, 00000014.00000003.444890733.0000000005230000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince	WerFault.exe, 00000014.00000003.444890733.0000000005230000.00000004.00000001.sdmp	false		high
http://https://corp.roblox.com/parents/	svchost.exe, 0000001B.00000003.494731203.00000193D751E000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.494312984.00000193D75AB000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.493537589.00000193D7566000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddress http://schemas.xmlsoap.org/ws/20	WerFault.exe, 00000014.00000003.444890733.0000000005230000.00000004.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000005.0000003.482507210.00000000812F000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcodehttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 00000014.00000003.444890733.0000000005230000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication	WerFault.exe, 00000014.00000003.444890733.0000000005230000.00000004.00000001.sdmp	false		high
http://www.g5e.com/G5_End_User_License_Supplemental_Terms	svchost.exe, 0000001B.00000003.462561929.00000193D7577000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.463207761.00000193D758D000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.462293843.00000193D756D000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x509distinguishednamehttp://schemas.xmlsoap.org/	WerFault.exe, 00000014.00000003.444890733.0000000005230000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	svchost.exe, 0000001F.00000002.644438974.000001F18E630000.00000002.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid	WerFault.exe, 00000014.00000003.444890733.0000000005230000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecisionhttp://schemas.xmlsoap.org/	WerFault.exe, 00000014.00000003.444890733.0000000005230000.00000004.00000001.sdmp	false		high
http://https://www.roblox.com/info/privacy	svchost.exe, 0000001B.00000003.494731203.00000193D751E000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.494312984.00000193D75AB000.00000004.00000001.sdmp	false		high
http://www.g5e.com/termsofservice	svchost.exe, 0000001B.00000003.462561929.00000193D7577000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.463207761.00000193D758D000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.462293843.00000193D756D000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/thumbprinthttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 00000014.00000003.444890733.0000000005230000.00000004.00000001.sdmp	false		high
http://https://en.help.roblox.com/hc/en-us	svchost.exe, 0000001B.00000003.494731203.00000193D751E000.00000004.00000001.sdmp, svchost.exe, 0000001B.00000003.494312984.00000193D75AB000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	WerFault.exe, 00000014.00000003.444890733.0000000005230000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.97.75	omaprillcode.duckdns.org	Netherlands		208476	DANILENKODE	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	411514
Start date:	11.05.2021
Start time:	23:52:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	y3t4g48gj6_PAYMENT.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:	36
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@32/27@3/3
EGA Information:	Failed
HDC Information:	- Successful, ratio: 5.5% (good quality ratio 0%) - Quality average: 0.3% - Quality standard deviation: 3.8%
HCA Information:	- Successful, ratio: 100% - 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 - Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 13.64.90.137, 92.122.145.220, 20.82.210.154, 92.122.213.194, 92.122.213.247, 93.184.221.240, 51.103.5.186, 52.155.217.156, 20.54.26.129, 40.126.31.141, 20.190.159.136, 20.190.159.134, 40.126.31.139, 20.190.159.138, 40.126.31.143, 40.126.31.4, 40.126.31.137, 52.255.188.83, 184.30.20.56, 168.61.161.212 - Excluded domains from analysis (whitelisted): store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, wu.azureedge.net, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skype-dataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skype-dataprdcolcus17.cloudapp.net, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, ris.api.iris.microsoft.com, skype-dataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, www.tm.lg.prod.aadmsa.trafficmanager.net - Execution Graph export aborted for target y3t4g48gj6_PAYMENT.exe, PID 6644 because there are no executed function - Execution Graph export aborted for target y3t4g48gj6_PAYMENT.exe, PID 7028 because it is empty - Report size exceeded maximum capacity and may have missing behavior information. - Report size getting too big, too many NtAllocateVirtualMemory calls found. - Report size getting too big, too many NtOpenKeyEx calls found. - Report size getting too big, too many NtQueryValueKey calls found. - Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
23:53:41	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce 51h0d2Kf8543fo5 C:\Windows\Resources\Themes\agcQ435Jh2M0514\svchost.exe
23:53:49	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce 51h0d2Kf8543fo5 C:\Windows\Resources\Themes\agcQ435Jh2M0514\svchost.exe
23:53:56	API Interceptor	805x Sleep call for process: y3t4g48gj6_PAYMENT.exe modified
23:54:22	API Interceptor	12x Sleep call for process: svchost.exe modified
23:54:22	API Interceptor	147x Sleep call for process: powershell.exe modified
23:54:51	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.97.75	IPUt7Nr2CH.exe	Get hash	malicious	Browse	
	q19CDiK5TD.exe	Get hash	malicious	Browse	
	d9hGzIR8mh.exe	Get hash	malicious	Browse	
	6554353_Payment_Invoice.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
omaprillcode.duckdns.org	IPUt7Nr2CH.exe	Get hash	malicious	Browse	• 194.5.97.75
	q19CDiK5TD.exe	Get hash	malicious	Browse	• 194.5.97.75

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	Quotation.jar	Get hash	malicious	Browse	• 194.5.98.38
	5lQuLT5Zu8.exe	Get hash	malicious	Browse	• 194.5.97.116
	IPUt7Nr2CH.exe	Get hash	malicious	Browse	• 194.5.97.75
	Passport_ID.jpg.jar	Get hash	malicious	Browse	• 194.5.98.228
	Vd80r7R7K5.exe	Get hash	malicious	Browse	• 194.5.98.208
	noVPhNP46G.exe	Get hash	malicious	Browse	• 194.5.98.208
	LQ0dDP64uk.exe	Get hash	malicious	Browse	• 194.5.98.208
	SCAN_DOCX-36673672.exe	Get hash	malicious	Browse	• 194.5.97.11
	4b092c1e_by_Libranalysis.docx	Get hash	malicious	Browse	• 194.5.98.208
	QW8lWJDpU8.exe	Get hash	malicious	Browse	• 194.5.98.5
	2a8f04dd_by_Libranalysis.docm	Get hash	malicious	Browse	• 194.5.98.210
	Invoice_orderYscFwfO1peuGI0w.exe	Get hash	malicious	Browse	• 194.5.98.250
	Quotation.jar	Get hash	malicious	Browse	• 194.5.97.87
	Quotation.jar	Get hash	malicious	Browse	• 194.5.97.87
	Quotation.jar	Get hash	malicious	Browse	• 194.5.97.87
	Quotation.jar	Get hash	malicious	Browse	• 194.5.97.87
	EFT payment.exe	Get hash	malicious	Browse	• 194.5.97.215
	Contract_Documents_pdf.exe	Get hash	malicious	Browse	• 194.5.98.203
	BANK DETAILS.jar	Get hash	malicious	Browse	• 194.5.97.87
	q19CDiK5TD.exe	Get hash	malicious	Browse	• 194.5.97.75

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5976804353698416
Encrypted:	false
SSDEEP:	6:btKVEk1GaD0JOCEfMuaaD0JOCEfMKQmDI0Al/gz2cE0fMbheZolrRSQ2hyYIIT:bYVrGaD0JcaaD0JwQQI0Ag/0bjSQJ
MD5:	C6A4D3B3B4EB755F99F9FD5B25FE88A9
SHA1:	343110136653D96FE8DFE258E50328777006AEC3
SHA-256:	7EDE1D0C07AD67C98AC68AD2D25206BC2CEC26F98D27AA0870170EA08BD63772
SHA-512:	D3F257F5229B0CCCA6740166296057F2D5E0E290AFB5C9D716EA6419BC39024937992357A5552AB7A44810AE0764B2452176559542AFECE7BB66946A55FC7927
Malicious:	false
Preview:	E..h..(....46...y.....1C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....46...y.....&.....e.f.3..w.....3..w.....h..C::\P.r.o.g.r.a.m .D.a.t.a.\M.i.c.r.o.s.o.f.t.\N.e.t.w.o.r.k.\D.o.w.n.l.o.a.d.e.r.\q.m.g.r..d.b...G.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0x80031985, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09616301549185044
Encrypted:	false
SSDEEP:	12:x0+Y1O4blqXOIRxKT0+Y1O4blqXOIRxK:q13lz13l
MD5:	E47EA999514BEC2CADE05C8F05257AE6
SHA1:	E685169FA7CF7F06FFF70FEE34C5A713E6CEBC1D
SHA-256:	7B6F583B5D70FE9AB6B695120C8DD5B615521F5F4FA5548F1D23E8595AF972C9
SHA-512:	D5E6ECD730C784F36EB3588103BBFAD79DDCBF821D5C9BA3355DD08547F92DA504B735BC6DDC0538E47C12F9F89E63038E7CB4A34A597A973D18E28F08B298C
Malicious:	false
Preview:	e.f.3..w.....&.....w..46...yG.h.{.....3..w.....B.....@.....3..w.....5.46...y.{.....5.46...yG.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.11086134938174995
Encrypted:	false
SSDEEP:	3:6TEvRriMuXI/bJdAtiLzvpCHYll:PJMA4lr
MD5:	D749BF4712C102699C1918F5266DFED0
SHA1:	6B0B812FA4903EF76603641A5A3CE3FEF5B2D9CF
SHA-256:	445AFA51E5E9610960E9B93176744416754E1CCF495F8A8C6FDE3FC6BD9971E6
SHA-512:	B708677FD5F6EC5B329394F52DEB276FAD880F669CE6E7A0A52E7D29DA7A83056E57BBF58E2CB62B2B285A4C7763723BA43952706AE75FD6B9F482145CB7AD22
Malicious:	false
Preview:	.m.=.....3..w..46...yG.....w.....w.....w.....O....w.....5..46...yG.....

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_y3t4g48gj6_PAYME_ce53192e427e57e166223ab89fc2d2b1ddc61e_5e276ace_16bcfe61\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	15294
Entropy (8bit):	3.7744507720065053
Encrypted:	false
SSDEEP:	192:O5sUrmHBUZMXyaKKIKZDnyK/u7sjS274ltjb:UISBUZMXyatyK/u7sjX4ltjb
MD5:	04B18104DC74E8A05B23CD669E5ADA60
SHA1:	6D30AAF091493A505269958BEF5D5ADDFa51D2C4
SHA-256:	BFEDFC3EC6F63C97FDB465DF9E9A32173937B26402D20570B26DDCC2CE2626BE
SHA-512:	D26968FC016564A690E8B3A08D3F8EB1C6B77A69ED3C1889C699E937ED74214639D2C01293F24412AA7AFF9C60CAFCDD05D153BE39F56101165D2DB81259FC18
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=1.....E.v.e.n.t.T.y.p.e.=C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=1.3.2.6.5.2.7.6.0.4.2.5.1.9.0.1.2.8.....R.e.p.o.r.t.T.y.p.e.=2.....C.o.n.s.e.n.t.=1.....U.p.l.o.a.d.T.i.m.e.=1.3.2.6.5.2.7.6.0.8.7.7.2.1.9.0.1.9.....R.e.p.o.r.t.S.t.a.t.u.s.=2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=3.1.e.7.a.7.b.7.-.8.f.2.0.-.4.0.9.5.-.8.3.3.f.-.3.1.f.a.0.a.e.7.e.d.3.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=7.0.a.2.9.b.4.f.-.f.f.1.c.-.4.0.4.7.-.8.1.9.3.-.4.1.f.7.c.a.8.f.d.a.f.f.....W.o.w.6.4.H.o.s.t.=3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=3.3.2.....N.s.A.p.p.N.a.m.e.=y.3.t.4.g.4.8.g.j.6__P.A.Y.M.E.N.T...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=v.a.l.u.e.i.n.f.i.n.i.t.e.V.M...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=0.0.0.0.1.b.7.4.-.0.0.0.1.-.0.0.1.7.-.a.a.4.e.-.3.a.7.e.f.b.4.6.d.7.0.1.....T.a.r.g.e.t.A.p.p.l.d.=W.:0.0.0.6.9.6.e.f.1.2.5.e.5.0.7.7.7.c.1.9.0.1.6.8.b.0.9.3.3.d.c.1.b.0.4.1.0.0.0.0.0.0.0.0.0.0.e.3.8.1.0.d.2.1.6.0.0.b.b.0.1.1.3.b.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER40BE.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed May 12 06:54:23 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	306847
Entropy (8bit):	3.8248011042062893
Encrypted:	false
SSDEEP:	3072:h59gJogF5Rso4g0aUCgUJVKMj7VTsNqktVfrT0ZN/jd+pROH2SDbUDYsck38i:h59RpDm9g5TjJYYBTRkrh0kpl9
MD5:	EF1B3D04FE6E9278638343B90563E41C
SHA1:	6A92CA503B4FB5A6BE57A69A14852F75766A3EF2
SHA-256:	508A49F23892320A01D50D2347C5553EA81F0C6ED774973687EB9F8A1F9C15B8
SHA-512:	1F457EEB4557F2B2FB569FFA317817A8E595EC79100EEBC7F14A9A94F84256D3C141FDE25B360C177A41ADCFF97DB10B46D32D716AB2D49ABEA869AE312F4353
Malicious:	false
Preview:	MDMP.....{.U.....B.....&.....GenuineIntelW.....T.....t.....{.0.....P.a.c.i.f.i.c..S.t.a.n.d.a.r.d..T.i.m.e.....P.a.c.i.f.i.c..D.a.y.l.i.g.h.t..T.i.m.e.....1.7.1.3.4..1...x.8.6.f.r.e...r.s.4..._r.e.l.e.a.s.e...1.8.0.4.1.0.-1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6...1.0...0..1.7.1.3.4..1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9EDD.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8438
Entropy (8bit):	3.7020515446608675
Encrypted:	false
SSDEEP:	192:Rr17r3GLNizN6M6YJVSU3w/jgmfZGSVCprn89bnasfONm:RrlsNiZ6M6YLSU3w/jgmf0S1n5fl
MD5:	D7FD4D77AE4CBE9D546552DCCBEB0454
SHA1:	72920FA887BB0257854AACFA05DEBD1E90F90BA4
SHA-256:	E38CA4B5A8F4BFDAC566326B67463984602897DBEEA95C865373BCA6E1111B4B
SHA-512:	22AD5E0D45975E285F3797E0F5ED689271C6694DB9D645B9B9D2BD95DB3E3A1AE44F2324BCBED75F5D7D02D08A6EE5DF2AC8BACFB229B1733133F1ECE721B6B
Malicious:	false
Preview:	..<?x.m.l..v.e.r.s.i.o.n.="1..0"..e.n.c.o.d.i.n.g.="U.T.F.-16"."?>.....<W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>1.0..0.</W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<B.u.i.l.d.>1.7.1.3.4.</B.u.i.l.d.>.....<P.r.o.d.u.c.t.>(0x30):. W.i.n.d.o.w.s..1.0..P.r.o.</P.r.o.d.u.c.t.>.....<E.d.i.t.i.o.n.>P.r.o.f.e.s.s.i.o.n.a.l.</E.d.i.t.i.o.n.>.....<B.u.i.l.d.S.t.r.i.n.g.>1.7.1.3.4..1...a.m.d.6.4.f.r.e...r.s.4..._r.e.l.e.a.s.e...1.8.0.4.1.0.-1.8.0.4.</B.u.i.l.d.S.t.r.i.n.g.>.....<R.e.v.i.s.i.o.n.>1.</R.e.v.i.s.i.o.n.>.....<F.l.a.v.o.r.>M.u.l.t.i.p.r.o.c.e.s.s.o.r..F.r.e.e.</F.l.a.v.o.r.>.....<A.r.c.h.i.t.e.c.t.u.r.e.>X.6.4.</A.r.c.h.i.t.e.c.t.u.r.e.>.....<L.C.I.D.>1.0.3.3.</L.C.I.D.>.....</O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<P.i.d.>7.0.2.8.</P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC2C.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4800
Entropy (8bit):	4.518003231098789

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC2C.tmp.xml	
Encrypted:	false
SSDEEP:	48:cvlwSD8zsgJgtWI9cyWSC8BS8fm8M4JGFFt+q8vNz9gmibkJBBed:ulTfmzTSN9JsKR9gsJBBed
MD5:	053F5DA168F81FB7A4F346AF2F12F765
SHA1:	D36D39E9B5F04BFEDE1A777C32DE750380C8FC7A
SHA-256:	FD185CEB967D561D88554F13718D3299F4413B6A8D754636445BBCAEBC433423
SHA-512:	C35BA475867E2729386C054B880A34260EC653C57160C08D35E671D9F046EF1FDC0AC61453FA718C6B4691AE9043641C96B6C8B2774A1419EE72402FFD1AF1BE
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>.<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verblid" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="985925" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC68.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	56240
Entropy (8bit):	3.053476393071879
Encrypted:	false
SSDEEP:	1536:XVHD3jxKN5MjZcr046S5Aevd5bUOtI+szgq1v62:XVHD3jxKN5MjZcr046S5Aevd5bU6l+sh
MD5:	5678794ED4AFADA5549ABF616FFE781A
SHA1:	F597D79405CCF2838712E49E9ED0F47296A0D8A6
SHA-256:	20A9F3450026F33C6A14425DA64E813BE81FC675D576693645B80553F9CC377A
SHA-512:	5042ACEEF8FBDCB657E6F008AE4C44811942DEDCCBC63679875E84C9CBDCADD0F55734823DEB9E3C60AD170DD8588FBF465A95EF110F00E0B36F7E6185DB173
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,H.a.r.d.F.a.u.l.t.C.o.u.n.t.,N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,C.y.c.l.e.T.i.m.e.,C.r.e.a.t.e.T.i.m.e.,U.s.e.r.T.i.m.e.,K.e.r.n.e.l.T.i.m.e.,B.a.s.e.P.r.i.o.r.i.t.y.,P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,V.i.r.t.u.a.l.S.i.z.e.,P.a.g.e.F.a.u.l.t.C.o.u.n.t.,W.o.r.k.i.n.g.S.e.t.S.i.z.e.,P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,P.a.g.e.f.i.l.e.U.s.a.g.e.,P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB87F.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6969687742225354
Encrypted:	false
SSDEEP:	96:9GiZYWkJ4L1OaYFYwWpeHQYEZw2jt5iEzqYs17waqFaUvh0Udzl0v3:9jZDkCSF2Kr+aUvhUO0v3
MD5:	BB8BBCD080A887F5B9E44281B318DB46
SHA1:	69AA6E5063EF1E3B86021EC996729AE3B2376C6F
SHA-256:	CF1FC5B4C3D7454352FD316293D1160565639466A3650A68CB49F058BF3016B2
SHA-512:	C0968E7C6D6ED008858112D28730B6605BCFB095D024E19D481EA904D7512348276DE727D4A1EED3B5619D786E5FE8D932CF2983E0A4E53952955B10E2251B94
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n.1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e.4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s.1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r.1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r.1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y.6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s.6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s.1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k.

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:cBV0GlpN6KQkj4iUxtaKdROdBLNXp5nYoGiB4J:cBV3lpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysis\Cache	
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-Scri pt.....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\Temp__PSScriptPolicyTest_elauq3ki.ml0.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ncewgnw3.qax.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_w14rpytb.25y.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_y12pedfd.ixi.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_y12pedfd.ixi.psm1	
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651C A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yw1y3y53.hqq.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651C A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_zah0ezrw.ehs.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651C A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\ID06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\ly3t4g48gj6_PAYMENT.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRNx/pBK0jCV83ne+VdWPiKgmR7kkmefoELBizbCuVkyYM:X4LDAAnybgCFcps0OafmCYDliZr/i/Oh
MD5:	9E7D0351E4DF94A9B0BADCEB6A9DB963
SHA1:	76C6A69B1C31CEA2014D1FD1E222A3DD1E433005
SHA-256:	AAFC7B40C5FE680A2BB549C3B90AABAAC63163F74FFFC0B00277C6BBFF88B757
SHA-512:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF385: 1
Malicious:	false
Preview:	Gj.h\3.A...5.x.&...i+...c(1.P..P.cLT...A.b.....4h...t+..Z\.. i... S....}FF.2...h.M+....L#.X..+.....*....~f.G0^.....W2:=-..K.-.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+ .2e"..E?.G.....[.&

C:\Users\user\AppData\Roaming\ID06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\ly3t4g48gj6_PAYMENT.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0

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



Encrypted:	false
SSDEEP:	3:Ej:Ej
MD5:	5B39604C071FE95CDDDD4F140631DDBCE
SHA1:	A2DA2E4C41AAC375127C23BB5E1083C95AEE156F
SHA-256:	E369706507154D1A34DC1D0A38E6AC34893B774936299A86EAA3EC708DE156F6
SHA-512:	934910C1F63D039492899A562F49C140DD1CCA7852FB049C6AC79E3EB1B039CB680110AEB91CE1ED051DFD69C6BC43460D5F3D1E7D88A354FE8FE7C9AE6DDC4
Malicious:	true
Preview:	(.R....H

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



Process:	C:\Users\user\Desktop\ly3t4g48gj6_PAYMENT.exe
File Type:	data
Category:	dropped
Size (bytes):	327768
Entropy (8bit):	7.999367066417797
Encrypted:	true
SSDEEP:	6144:oX44S90aTiB66x3PIZmqze1d1w8lkWmtjJ/3Exi:LkjbU7LjGxi
MD5:	2E52F446105FBF828E63CF808B721F9C
SHA1:	5330E54F238F46DC04C1AC62B051DB4FCD7416FB
SHA-256:	2F7479AA2661BD259747BC89106031C11B3A3F79F12190E7F19F5DF65B7C15C8
SHA-512:	C08BA0E3315E2314ECBEF38722DF834C2CB8412446A9A310F41A8F83B4AC5984FCC1B26A1D8B0D58A730FDBDD885714854BDFD04DCDF7F582FC125F552D5C3A
Malicious:	false
Preview:	pT...l..W..G..J..a..).@i..wpk..so@...5.=^..Q..oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~... .fX_...Xf.p^.....>a..\$...e.6:7d.(a.A...=)*.....{B.[...y%*.i.Q<..xt.X..H.. ..H F7g...l.*3.{.n....L.y;i..s-...(5i.....J.5b7)..fK..HV.....0.... ..n.w6PMI.....v.""v.....#.X.a...../..cC...i..l[>5n._+e.d'...)[.../...D.t.GVp.zz.....(..o.....b...+J.{...hS1G.^*l..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.I.K.w"o..E..."K%{...z.7....<.....}t.....[.Z.u...3X8.Ql..j_&..N..q.e.2...6.R.~..9.Bq..A.v.6.G.#y.....O...Z)G...w..E..k(...+.O.....Vg.2xC.... .O...jc.....z..~.P...q./.-'.h..._cj=..B.x.Q9.pu.l[i4...i...;O...n.?.,.v?5).OY@.dG <.._69@.2..m..l..oP=...xrK.?.....b..5....i&...l.c b).Q..O+.V.mJ....pz....>F.....H...6\$. ..d... m...N...1.R..B.i.....\$...\$.....CY)..\$.r.....H...8...l.....7 P.....?h...R.i.F..6...q{.@Ll.s..+K.....?m..H....*. l.<}>.... .B....3.....l..o...u1..8i=z.W..7

C:\Users\user\Documents\20210511\PowerShell_transcript.878411.68FOB_yb.20210511235334.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):	5217
Entropy (8bit):	5.417695523418659
Encrypted:	false
SSDEEP:	96:BZJTLLNq1qDo1Z7ZTLLNq1qDo1Zp8D+DEDjZGTLNq1qDo1ZgvD0D9:n
MD5:	CFB4E49471003BAA780AACF9AC7FFD87
SHA1:	D8B217E2716AF6E9661D7FFA87DB3EE0BD475549
SHA-256:	8963C4AAE1D6854EF7D7B0D1E71529A44B2514E8AF40BC1919B1EEE3C93FA04C
SHA-512:	482B86E1AD26B7198A4BFCADCACCF9301D0F6258C982AC304441BCAFE07FE6BF0F736787E44920143A6C941A11F19FECDD68COC6F54D45F8D8F3B32652A84C18
Malicious:	false
Preview:	*****. Windows PowerShell transcript start..Start time: 20210511235359..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 878411 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Windows\Resources\Themes\agcQ435Jh2M0514\svchost.exe -Force..Process ID: 4668..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: 20210511235400. *****..PS>Add-MpPreference -ExclusionPath C:\Windows\Resources\Themes\agcQ435Jh2M0514\svchost.exe -Force..*****. Windows PowerShell transcript start..Start time: 20210512000222..Username: computer

C:\Users\user\Documents\20210511\PowerShell_transcript.878411.E9GVYDVQ.20210511235337.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):	1586
Entropy (8bit):	5.33741245385722
Encrypted:	false
SSDEEP:	48:BZMwvTLLoO+SWsXqDYB1Z6cW2ZYhvTLLoO+SWsXqDYB1ZA:BZMITLLNqYqDo1Z6J2ZATLLNqYqDo1ZA
MD5:	24B7153068B74F63D00506BD762CF0AF
SHA1:	F695E04DD31E7CCF7566E3F433A74E151E79AE32
SHA-256:	1BC99D330DB74DC6B97DC17D234CE3B318168E992DDC1096B597491B2D5C7D29
SHA-512:	AF36DF4F7BDF35A6C3F1CBF0F0E9472952A459C536B29EF1C14536E1213D5525641E56A5B9DD49EA1CF8F99B46970686DCE656494637AB7E797CCDD2BB8B8C0F
Malicious:	false

C:\Users\user\Documents\20210511\PowerShell_transcript.878411.ZQ4X65kJ.20210511235337.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):	4309
Entropy (8bit):	5.442531877682068
Encrypted:	false
SSDEEP:	96:BZ5NTLLN+qDo1ZJZPTLLN+qDo1Zlc+0jZTLLN+qDo1ZVe:IU
MD5:	8A5EA0648FDE1D231A3B3F62DFF232E0
SHA1:	09463333CC5CEA72630A6F59E4128B60822C2D53
SHA-256:	41D5A08E8E4022B1319554A9B6DB233E0FBBB187F7BB87C74D3DC69CC68421DF
SHA-512:	9F88C010951C5D619A97F310094086CC1252B2B2C39B87254ECCA0730BE208CAD81A73743055119F7EDA31FE2111CD07D9F201993DFD11415E50AD962089EB2
Malicious:	false
Preview:	<pre> *****.Windows PowerShell transcript start..Start time: 20210511235403..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 878411 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference - ExclusionPath C:\Users\user\Desktop\3t4g48gj6_PAYMENT.exe -Force..Process ID: 4896..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: 20210511235404.*****.PS>Add-MpPreference -ExclusionPath C:\Users\user \Desktop\3t4g48gj6_PAYMENT.exe -Force..*****.Windows PowerShell transcript start..Start time: 20210512000244..Username: computer\user..Run </pre>

C:\Windows\Resources\Themes\agcQ435Jh2M0514\svchost.exe	
Process:	C:\Users\user\Desktop\ly3t4g48gj6_PAYMENT.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3867176
Entropy (8bit):	2.590642055759663
Encrypted:	false
SSDEEP:	24576:Bg2krlcNk1WgwmNHtf+Gqwqf/JOy0h1qMEIGCjx9h3CIf9rMRrdA7w1cYAnXs6M7:Bh
MD5:	9998F7E0C708BA1FA4B56235A9811C0F
SHA1:	E3810D21600BB0113B2D7116347326BEB6A35D83
SHA-256:	9F44F33F1B0B724292959B65AE6F2918CB1993641AD7832FFDBD68FC00FDDA2C
SHA-512:	69A0FEA89ADC2F259624E6ABA5CF20194A904E8656444DF6894785775F57DAEC33AB08903D5147152482D7CFAAFF91C30FA51965FE472EB1E91DF42B709432F2
Malicious:	true
Antivirus:	- Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: ReversingLabs, Detection: 15%
Preview:	<pre> MZ.....@.....!..L!This program cannot be run in DOS mode...\$......PE..L...%Y....."....0.....;... ..;...@.....`.....5S; ..@.....;O...;.....:([@:......H.....text...4... ..;......rsrc.....;.....@...@.rel oc.....@.....@..B......H.....\$. :.....#. ...".f...D.....(....0...\$.....+...*.0.....~...+...*.0.....~...+...*.0.....(....+...+.....*0.9.....f.:p+.....(....(....(.....%.. .0.....+L.....f.:p(.....+*.0.....+.....(....~.....0.....X.. </pre>

C:\Windows\Resources\Themes\agcQ435Jh2M0514\svchost.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\ly3t4g48gj6_PAYMENT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	true
Preview:	[ZoneTransfer].....Zoneld=0

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRI83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	2.590642055759663
TrID:	- Win32 Executable (generic) Net Framework (10011505/4) 50.01% - Win32 Executable (generic) a (10002005/4) 49.97% - Generic Win/DOS Executable (2004/3) 0.01% - DOS Executable Generic (2002/1) 0.01% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	y3t4g48gj6_PAYMENT.exe
File size:	3867176
MD5:	9998f7e0c708ba1fa4b56235a9811c0f
SHA1:	e3810d21600bb0113b2d7116347326beb6a35d83
SHA256:	9f44f33f1b0b724292959b65ae6f2918cb1993641ad7832f fdbd68fc00fdda2c
SHA512:	69a0fea89adc2f259624e6aba5cf20194a904e8656444df 6894785775f57daec33ab08903d5147152482d7cfaaff91 c30fa51965fe472eb1e91df42b709432f2
SSDEEP:	24576:Bg2krlcNk1WgwmNHtf+Gqwqf/JOy0h1qMEIGCj x9h3CIf9rMRrdA7w1cYAnXs6M7:Bh
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$......PE..L.. %Y.....".....0.....;.....@.....;.....5 S;...@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x7b032e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xD9F65925 [Sat Nov 17 01:55:49 2085 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4

General	
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	false
Signature Issuer:	C=by64bc71k4HZ0Yw5C4bba6cc73Yfz0a, S=H9a5205c91ku3, L=5Jp25b35, T=NweE2NdNRd1J7Jb5wDdffe141z527c2ci41dgw3, E=4rhdU4t04, OU=484d0C6323bzd4c97q3, O=bR673KfoLs612894halpX4a4d0qGA2d583, CN=44QI7muB5F53555J17d1o
Signature Validation Error:	A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider
Error Number:	-2146762487
Not Before, Not After	5/11/2021 7:54:44 AM 5/11/2022 7:54:44 AM
Subject Chain	C=by64bc71k4HZ0Yw5C4bba6cc73Yfz0a, S=H9a5205c91ku3, L=5Jp25b35, T=NweE2NdNRd1J7Jb5wDdffe141z527c2ci41dgw3, E=4rhdU4t04, OU=484d0C6323bzd4c97q3, O=bR673KfoLs612894halpX4a4d0qGA2d583, CN=44QI7muB5F53555J17d1o
Version:	3
Thumbprint MD5:	987431C54CFEF315C111B5AB521BCAC1
Thumbprint SHA-1:	DD65EBFE2F0AF6EC396DC73C4A037E87E321A06B
Thumbprint SHA-256:	93C6C15FCE022D65F38E693A5BADB285F2BE5AC5EC2BFC2707FBB16E192C6E96
Serial:	00BEABD3255E63776CE32FBB6B780B4783

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 [5], al

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

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

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

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

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

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

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

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

add byte ptr [eax], al

add byte ptr [eax], al

add byte ptr [eax], al

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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


Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3b02dc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b2000	0x5d8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x3aee00	0x1428	.text
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3b4000	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	0x3ae334	0x3ae400	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x3b2000	0x5d8	0x600	False	0.421223958333	data	4.14589146106	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x3b4000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x3b20a0	0x34c	data		
RT_MANIFEST	0x3b23ec	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	Copyright 2021
Assembly Version	1.0.0.0
InternalName	valueinfiniteVM.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	valueinfiniteVM
ProductVersion	1.0.0.0
FileDescription	valueinfiniteVM
OriginalFilename	valueinfiniteVM.exe

Network Behavior

Network Port Distribution

Total Packets: 84

- 53 (DNS)
- 8090 undefined



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 23:54:01.991233110 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:02.134605885 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:02.135693073 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:02.315650940 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:02.478807926 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:02.480408907 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:02.671775103 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:02.672080994 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:02.816175938 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:02.863444090 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:02.887123108 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.079195976 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.126389980 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.126424074 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.126483917 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.126511097 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.126547098 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.126751900 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.269855022 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.269893885 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.269922018 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.270036936 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.270086050 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.270333052 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.270370007 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.270394087 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.270730972 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.270766020 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.270853996 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.271909952 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.411948919 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.413635969 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.413660049 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.413749933 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.413784027 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.413881063 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.414004087 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.414113998 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.414186954 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.414292097 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.414758921 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.414782047 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.414894104 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.414992094 CEST	8090	49735	194.5.97.75	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 23:54:03.415210009 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.415313005 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.415316105 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.415663004 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.415685892 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.415707111 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.415882111 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.415919065 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.416126013 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.416162968 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.416321039 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.416354895 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.416470051 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.416507959 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.416852951 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.559678078 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.559794903 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.559885979 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.560215950 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.560280085 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.560347080 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.560524940 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.560698032 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.560772896 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.560782909 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.561068058 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.561141014 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.561413050 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.561588049 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.561609030 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.561693907 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.561811924 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.561887026 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.562055111 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.562211037 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.562280893 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.562416077 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.562525988 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.562608957 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.562710047 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.562809944 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.562887907 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.562964916 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.563091993 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.563165903 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.563282967 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.563446045 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.563523054 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.563656092 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.563893080 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.564035892 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.564192057 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.564239979 CEST	49735	8090	192.168.2.6	194.5.97.75
May 11, 2021 23:54:03.564415932 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.564444065 CEST	8090	49735	194.5.97.75	192.168.2.6
May 11, 2021 23:54:03.564467907 CEST	49735	8090	192.168.2.6	194.5.97.75

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 23:53:12.693845987 CEST	53	64267	8.8.8.8	192.168.2.6
May 11, 2021 23:53:13.288600922 CEST	49448	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:13.337548971 CEST	53	49448	8.8.8.8	192.168.2.6
May 11, 2021 23:53:13.768048048 CEST	60342	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 23:53:13.826888084 CEST	53	60342	8.8.8.8	192.168.2.6
May 11, 2021 23:53:14.419569016 CEST	61346	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:14.468420982 CEST	53	61346	8.8.8.8	192.168.2.6
May 11, 2021 23:53:15.593247890 CEST	51774	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:15.641983986 CEST	53	51774	8.8.8.8	192.168.2.6
May 11, 2021 23:53:16.709300995 CEST	56023	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:16.760977030 CEST	53	56023	8.8.8.8	192.168.2.6
May 11, 2021 23:53:18.120974064 CEST	58384	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:18.178188086 CEST	53	58384	8.8.8.8	192.168.2.6
May 11, 2021 23:53:19.353452921 CEST	60261	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:19.410451889 CEST	53	60261	8.8.8.8	192.168.2.6
May 11, 2021 23:53:20.766933918 CEST	56061	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:20.821878910 CEST	53	56061	8.8.8.8	192.168.2.6
May 11, 2021 23:53:22.508728981 CEST	58336	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:22.566011906 CEST	53	58336	8.8.8.8	192.168.2.6
May 11, 2021 23:53:23.694828987 CEST	53781	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:23.744986057 CEST	53	53781	8.8.8.8	192.168.2.6
May 11, 2021 23:53:25.092776060 CEST	54064	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:25.144562006 CEST	53	54064	8.8.8.8	192.168.2.6
May 11, 2021 23:53:26.295615911 CEST	52811	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:26.344513893 CEST	53	52811	8.8.8.8	192.168.2.6
May 11, 2021 23:53:27.467045069 CEST	55299	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:27.524247885 CEST	53	55299	8.8.8.8	192.168.2.6
May 11, 2021 23:53:28.619930983 CEST	63745	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:28.668901920 CEST	53	63745	8.8.8.8	192.168.2.6
May 11, 2021 23:53:29.828959942 CEST	50055	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:29.880475044 CEST	53	50055	8.8.8.8	192.168.2.6
May 11, 2021 23:53:30.955908060 CEST	61374	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:31.015707016 CEST	53	61374	8.8.8.8	192.168.2.6
May 11, 2021 23:53:32.130070925 CEST	50339	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:32.190007925 CEST	53	50339	8.8.8.8	192.168.2.6
May 11, 2021 23:53:35.031847954 CEST	63307	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:35.083312035 CEST	53	63307	8.8.8.8	192.168.2.6
May 11, 2021 23:53:38.200325966 CEST	49694	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:38.248883963 CEST	53	49694	8.8.8.8	192.168.2.6
May 11, 2021 23:53:47.785288095 CEST	54982	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:47.842583895 CEST	53	54982	8.8.8.8	192.168.2.6
May 11, 2021 23:53:52.343401909 CEST	50010	53	192.168.2.6	8.8.8.8
May 11, 2021 23:53:52.402043104 CEST	53	50010	8.8.8.8	192.168.2.6
May 11, 2021 23:54:01.630276918 CEST	63718	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:01.852056026 CEST	53	63718	8.8.8.8	192.168.2.6
May 11, 2021 23:54:08.121082067 CEST	62116	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:08.183593035 CEST	53	62116	8.8.8.8	192.168.2.6
May 11, 2021 23:54:09.129223108 CEST	63816	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:09.188091040 CEST	53	63816	8.8.8.8	192.168.2.6
May 11, 2021 23:54:15.967436075 CEST	55014	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:16.193136930 CEST	53	55014	8.8.8.8	192.168.2.6
May 11, 2021 23:54:20.714508057 CEST	62208	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:20.841531992 CEST	53	62208	8.8.8.8	192.168.2.6
May 11, 2021 23:54:21.201359987 CEST	57574	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:21.258441925 CEST	53	57574	8.8.8.8	192.168.2.6
May 11, 2021 23:54:22.554590940 CEST	51818	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:22.611522913 CEST	53	51818	8.8.8.8	192.168.2.6
May 11, 2021 23:54:23.394865990 CEST	56628	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:23.454391003 CEST	53	56628	8.8.8.8	192.168.2.6
May 11, 2021 23:54:24.354697943 CEST	60778	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:24.413964987 CEST	53	60778	8.8.8.8	192.168.2.6
May 11, 2021 23:54:26.336348057 CEST	53799	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:26.441319942 CEST	53	53799	8.8.8.8	192.168.2.6
May 11, 2021 23:54:27.199091911 CEST	54683	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:27.257597923 CEST	53	54683	8.8.8.8	192.168.2.6
May 11, 2021 23:54:27.711756945 CEST	59329	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:27.769222021 CEST	53	59329	8.8.8.8	192.168.2.6
May 11, 2021 23:54:31.061930895 CEST	64021	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 23:54:31.122121096 CEST	53	64021	8.8.8.8	192.168.2.6
May 11, 2021 23:54:33.969976902 CEST	56129	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:34.032226086 CEST	53	56129	8.8.8.8	192.168.2.6
May 11, 2021 23:54:38.607516050 CEST	58177	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:38.667622089 CEST	53	58177	8.8.8.8	192.168.2.6
May 11, 2021 23:54:40.595410109 CEST	50700	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:40.644227028 CEST	53	50700	8.8.8.8	192.168.2.6
May 11, 2021 23:54:42.386462927 CEST	54069	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:42.443860054 CEST	53	54069	8.8.8.8	192.168.2.6
May 11, 2021 23:54:49.005872965 CEST	61178	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:49.086483955 CEST	53	61178	8.8.8.8	192.168.2.6
May 11, 2021 23:54:50.037343979 CEST	57017	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:50.087301970 CEST	53	57017	8.8.8.8	192.168.2.6
May 11, 2021 23:54:53.723217964 CEST	56327	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:53.783620119 CEST	53	56327	8.8.8.8	192.168.2.6
May 11, 2021 23:54:54.585988998 CEST	50243	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:54.654728889 CEST	53	50243	8.8.8.8	192.168.2.6
May 11, 2021 23:54:55.628778934 CEST	62055	53	192.168.2.6	8.8.8.8
May 11, 2021 23:54:55.687485933 CEST	53	62055	8.8.8.8	192.168.2.6
May 11, 2021 23:55:48.602257967 CEST	61249	53	192.168.2.6	8.8.8.8
May 11, 2021 23:55:48.659320116 CEST	53	61249	8.8.8.8	192.168.2.6
May 11, 2021 23:55:48.808475018 CEST	65252	53	192.168.2.6	8.8.8.8
May 11, 2021 23:55:48.865681887 CEST	53	65252	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 11, 2021 23:54:01.630276918 CEST	192.168.2.6	8.8.8.8	0xc28b	Standard query (0)	omaprilcode.duckdns.org	A (IP address)	IN (0x0001)
May 11, 2021 23:54:15.967436075 CEST	192.168.2.6	8.8.8.8	0x2bd2	Standard query (0)	omaprilcode.duckdns.org	A (IP address)	IN (0x0001)
May 11, 2021 23:54:23.394865990 CEST	192.168.2.6	8.8.8.8	0x3fa7	Standard query (0)	omaprilcode.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

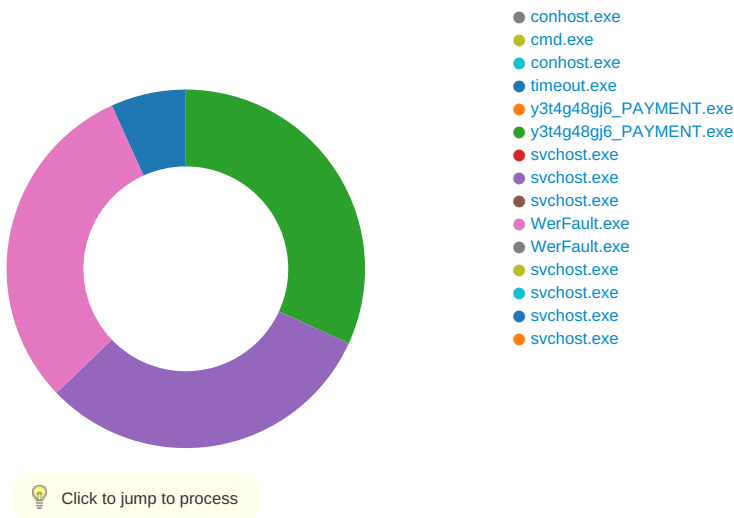
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 23:54:01.852056026 CEST	8.8.8.8	192.168.2.6	0xc28b	No error (0)	omaprilcode.duckdns.org		194.5.97.75	A (IP address)	IN (0x0001)
May 11, 2021 23:54:16.193136930 CEST	8.8.8.8	192.168.2.6	0x2bd2	No error (0)	omaprilcode.duckdns.org		194.5.97.75	A (IP address)	IN (0x0001)
May 11, 2021 23:54:23.454391003 CEST	8.8.8.8	192.168.2.6	0x3fa7	No error (0)	omaprilcode.duckdns.org		194.5.97.75	A (IP address)	IN (0x0001)
May 11, 2021 23:54:49.086483955 CEST	8.8.8.8	192.168.2.6	0x7418	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

- y3t4g48gj6_PAYMENT.exe
- svchost.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- powershell.exe



System Behavior

Analysis Process: y3t4g48gj6_PAYMENT.exe PID: 7028 Parent PID: 5908

General

Start time:	23:53:20
Start date:	11/05/2021
Path:	C:\Users\user\Desktop\y3t4g48gj6_PAYMENT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\y3t4g48gj6_PAYMENT.exe'
Imagebase:	0xfc0000
File size:	3867176 bytes
MD5 hash:	9998F7E0C708BA1FA4B56235A9811C0F
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: 00000001.00000002.600696980.00000000046E1000.00000004.00000001.sdmp, Author: Florian Roth - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.600696980.00000000046E1000.00000004.00000001.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000001.00000002.600696980.00000000046E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\Resources\Themes\agcQ435Jh2M0514	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6CBCBEFF	CreateDirectoryW
C:\Windows\Resources\Themes\agcQ435Jh2M0514\svchost.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	6CBCDD66	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\Resources\Themes\agcQ435Jh2M0514\svchost.exe\Zone.Identifier:\$DATA	read data or list directory synchronize generic write	device	sequential only synchronous io non alert	success or wait	1	6CBCDD66	CopyFileW
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	6DD7CF06	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	6DD7CF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Resources\Themes\lag cQ435Jh2M0514\svchost.exe	0	524288	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 \$.....PE..L...%Y..... 00 00 00 00 00 00 00 "...0...:... ;...@.. 00 00 00 00 00 00 00 ;....SS;...@..... 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 25 59 f6 d9 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 e4 3a 00 00 08 00 00 00 00 00 00 2e 03 3b 00 00 20 00 00 00 20 3b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 3b 00 00 02 00 00 35 53 3b 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...%Y..... "...0...:... ;...@..` ;....SS;...@.....	success or wait	8	6CBCDD66	CopyFileW
C:\Windows\Resources\Themes\lag cQ435Jh2M0514\svchost.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	6CBCDD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorliba152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba49ab6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	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	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0_0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DD3D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0_0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DD3D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6DD3D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6DD3D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll	unknown	4096	success or wait	1	6DD3D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll	unknown	512	success or wait	1	6DD3D72F	unknown
C:\Users\user\Desktop\3t4g48gj6_PAYMENT.exe	unknown	4096	success or wait	1	6DD3D72F	unknown
C:\Users\user\Desktop\3t4g48gj6_PAYMENT.exe	unknown	512	success or wait	1	6DD3D72F	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	6CBC5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6CBC5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6CBC5F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Windows\Resources\Themes\lagcQ435Jh2M0514\svchost.exe	dword	0	success or wait	1	6BCC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\Desktop\3t4g48gj6_PAYMENT.exe	dword	0	success or wait	1	6BCC075	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	51h0d2Kf8543fo5	unicode	C:\Windows\Resources\Themes\lagcQ435Jh2M0514\svchost.exe	success or wait	1	6CBC646A	RegSetValueExW

Analysis Process: svchost.exe PID: 7128 Parent PID: 560

General

Start time:	23:53:23
Start date:	11/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: powershell.exe PID: 4668 Parent PID: 7028

General

Start time:	23:53:31
Start date:	11/05/2021
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:\Windows\Resources\Themes\lagcQ435Jh2M0514\svchost.exe' -Force
Imagebase:	0xd30000
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	6DD7CF06	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	6DD7CF06	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	6CB25B28	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	6CB25B28	unknown
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_yw1y3y53.hqg.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6CBC1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_w14rpytb.25y.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6CBC1E60	CreateFileW
C:\Users\user\Documents\20210511	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6CBCBEFF	CreateDirectoryW
C:\Users\user\Documents\20210511\PowerShell_transcr ipt.878411.68FOB_yb.20210511235334.txt	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	6CBC1E60	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	6CBC1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yw1y3y53.hgg.ps1	success or wait	1	6CBC6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_w14rpytb.25y.psm1	success or wait	1	6CBC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_yw1y3y53.hqq.ps1	unknown	1	31	1	success or wait	1	6CBC1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscr iptPolicyTest_w14rpytb.25y.psm1	unknown	1	31	1	success or wait	1	6CBC1B4F	WriteFile
C:\Users\user\Documents\20210511\PowerShell_transcr ipt.878411.68FOB_yb.20210511235334.txt	unknown	3	ef bb bf	...	success or wait	1	6CBC1B4F	WriteFile
C:\Users\user\Documents\20210511\PowerShell_transcr ipt.878411.68FOB_yb.20210511235334.txt	unknown	700	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 35 31 31 32 33 35 33 35 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 65 6e 67 69 6e 65 65 72 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 65 6e 67 69 6e 65 65 72 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 38 37 38 34 31 31 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	*****.Windows PowerShell transcript start..Start time: 20210511235359..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 878411 (Microsoft Windows NT 10.0.17134.0)..Host Application:	success or wait	30	6CBC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 77 dc 65 ca 9f d5 08 61 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 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 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 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....w. e.....a...C:\Program Files (x86)\Windows PowerShell\Modules\Pack ageMana gement\1.0.0.1\PackageM anagement.psd1.....Set- PackageSour ce.....Unregister- PackageSource.....Get- PackageSource.Install-Package..... Save-Package...	success or wait	2	6CBC1B4F	WriteFile
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\PowerShellG et\1.0.0.1\PowerShellGet.p sd1.....Uninstall- Module..... .inmo.....fimo.....Install- Module.....New-scr iptFileInfo.....Publish- Module.....Install-Sc	success or wait	1	6CBC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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-Runspace	success or wait	1	6CBC1B4F	WriteFile
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	6CBC1B4F	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	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD55705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorliba152fe02a317a77aeec36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD5CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD55705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DD61F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21316	success or wait	1	6DD6203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCB03DE	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	6CBC1B4F	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	6CBC1B4F	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	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefaf3cd3e0ba98b5ebddb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CBC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	8	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CBC1B4F	ReadFile

Analysis Process: conhost.exe PID: 4104 Parent PID: 4668

General

Start time:	23:53:32
Start date:	11/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 4896 Parent PID: 7028

General

Start time:	23:53:32
Start date:	11/05/2021
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\3t4g48gj6_PAYMENT.exe' -Force
Imagebase:	0xd30000
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	6DD7CF06	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	6DD7CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ncewgnw3.qax.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6CBC1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zah0ezrw.ehs.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6CBC1E60	CreateFileW
C:\Users\user\Documents\20210511\PowerShell_transcript.878411.ZQ4X65kJ.20210511235337.txt	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	6CBC1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ncewgnw3.qax.ps1	success or wait	1	6CBC6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zah0ezrw.ehs.psm1	success or wait	1	6CBC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ncewgnw3.qax.ps1	unknown	1	31	1	success or wait	1	6CBC1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zah0ezrw.ehs.psm1	unknown	1	31	1	success or wait	1	6CBC1B4F	WriteFile
C:\Users\user\Documents\20210511\PowerShell_transcript.878411.ZQ4X65kJ.20210511235337.txt	unknown	3	ef bb bf	...	success or wait	1	6CBC1B4F	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\PowerShellG et\1.0.0.1\PowerShellGet.p sd1.....Uninstall- Module..... .inmo.....fimo.....Install- Module.....New-scr iptFileInfo.....Publish- Module.....Install-Sc	success or wait	1	6CBC1B4F	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-Runspace	success or wait	1	6CBC1B4F	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 5f 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- PackageProvid er.....Import- PackageProvider.....Get- PackageProvider.Register- PackageSource.Uninstall-Package..... ..Find- PackageProvider.....I...C:\Windows\syste m3 2\WindowsPowerShell\1. 0\Modules\Defender\Def	success or wait	1	6CBC1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\1.0\powershell.exe.config	unknown	8173	end of file	1	6DD5CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD55705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DD61F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21316	success or wait	1	6DD6203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCB03DE	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	6CBC1B4F	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	6CBC1B4F	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	6CBC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	2	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	138	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mif49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	8	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CBC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CBC1B4F	ReadFile

Analysis Process: conhost.exe PID: 4524 Parent PID: 4896

General

Start time:	23:53:32
Start date:	11/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 1912 Parent PID: 7028

General

Start time:	23:53:32
Start date:	11/05/2021
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:\Windows\Resources\Themes\agcQ435Jh2M0514\svchost.exe' -Force
Imagebase:	0xd30000
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	6DD7CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6DD7CF06	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	6CB25B28	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	6CB25B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_elauq3ki.ml0.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6CBC1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y12pedfd.ixi.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6CBC1E60	CreateFileW
C:\Users\user\Documents\20210511\PowerShell_transcript.878411.E9GVYDVQ.20210511235337.txt	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	6CBC1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_elauq3ki.ml0.ps1	success or wait	1	6CBC6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y12pedfd.ixi.psm1	success or wait	1	6CBC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscri iptPolicyTest_elauq3ki.ml0.ps1	unknown	1	31	1	success or wait	1	6CBC1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscri iptPolicyTest_y12pedfd.ixi.psm1	unknown	1	31	1	success or wait	1	6CBC1B4F	WriteFile
C:\Users\user\Documents\20210511\PowerShell_transcr ipt.878411.E9GVYDVQ.20210511235337.txt	unknown	3	ef bb bf	...	success or wait	1	6CBC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210511\PowerShell_transcript.878411.E9GVYDVQ.20210511235337.txt	unknown	700	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 35 31 31 32 33 35 34 31 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 65 6e 67 69 6e 65 65 72 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 65 6e 67 69 6e 65 65 72 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 38 37 38 34 31 31 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	*****..Windows PowerShell transcript start..Start time: 20210511235410..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 878411 (Microsoft Windows NT 10.0.17134.0)..Host Application:	success or wait	6	6CBC1B4F	WriteFile
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\et\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module......inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6CBC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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-Runspace	success or wait	1	6CBC1B4F	WriteFile
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 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	6CBC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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- BitLockerRequiredActi onsInternal.....Unlock- Pass wordInternal.....Unlock- BitLocker.....Add- TpmProtector Internal....%...Add- RecoveryPa sswordProtectorInternal..... ...Unlock-Recover	success or wait	1	6CBC1B4F	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	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DCB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD5CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD55705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DD61F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21316	success or wait	1	6DD6203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCB03DE	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	6CBC1B4F	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	6CBC1B4F	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	6CBC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	130	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CBC1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7f093d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DCB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DCB03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	4	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DD55705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	10	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CBC1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CBC1B4F	ReadFile

Analysis Process: conhost.exe PID: 6408 Parent PID: 1912

General

Start time:	23:53:33
Start date:	11/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: cmd.exe PID: 6336 Parent PID: 7028

General

Start time:	23:53:38
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6356 Parent PID: 6336

General

Start time:	23:53:38
Start date:	11/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: timeout.exe PID: 4752 Parent PID: 6336

General	
Start time:	23:53:38
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0xa90000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: y3t4g48gj6_PAYMENT.exe PID: 6644 Parent PID: 7028

General	
Start time:	23:53:44
Start date:	11/05/2021
Path:	C:\Users\user\Desktop\y3t4g48gj6_PAYMENT.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\y3t4g48gj6_PAYMENT.exe
Imagebase:	0x240000
File size:	3867176 bytes
MD5 hash:	9998F7E0C708BA1FA4B56235A9811C0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: y3t4g48gj6_PAYMENT.exe PID: 6868 Parent PID: 7028

General	
Start time:	23:53:47
Start date:	11/05/2021
Path:	C:\Users\user\Desktop\y3t4g48gj6_PAYMENT.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\y3t4g48gj6_PAYMENT.exe
Imagebase:	0xa50000
File size:	3867176 bytes
MD5 hash:	9998F7E0C708BA1FA4B56235A9811C0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: svchost.exe PID: 7088 Parent PID: 560

General	
Start time:	23:53:48
Start date:	11/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p

Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6824 Parent PID: 3440

General

Start time:	23:53:49
Start date:	11/05/2021
Path:	C:\Windows\Resources\Themes\agcQ435Jh2M0514\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Resources\Themes\agcQ435Jh2M0514\svchost.exe'
Imagebase:	0x70000
File size:	3867176 bytes
MD5 hash:	9998F7E0C708BA1FA4B56235A9811C0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	- Detection: 100%, Joe Sandbox ML - Detection: 15%, ReversingLabs
Reputation:	low

Analysis Process: svchost.exe PID: 4696 Parent PID: 560

General

Start time:	23:53:52
Start date:	11/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 6396 Parent PID: 4696

General

Start time:	23:53:52
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 7028 -ip 7028
Imagebase:	0x1360000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 5760 Parent PID: 7028

General

Start time:	23:53:55
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7028 -s 1780
Imagebase:	0x1360000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 5980 Parent PID: 3440

General

Start time:	23:53:58
Start date:	11/05/2021
Path:	C:\Windows\Resources\Themes\agcQ435Jh2M0514\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Resources\Themes\agcQ435Jh2M0514\svchost.exe'
Imagebase:	0xc10000
File size:	3867176 bytes
MD5 hash:	9998F7E0C708BA1FA4B56235A9811C0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 6160 Parent PID: 560

General

Start time:	23:54:03
Start date:	11/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5280 Parent PID: 560

General

Start time:	23:54:18
-------------	----------

Start date:	11/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 2032 Parent PID: 560

General

Start time:	23:54:51
Start date:	11/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis