ID: 403532
Sample Name: 741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe
Cookbook: default.jbs
Time: 07:14:23
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report 741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.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
System Summary: 7
Signature Overview 7
AV Detection: 8
Networking: 8
E-Banking Fraud: 8
System Summary: 8
Data Obfuscation: 8
Boot Survival: 8
Hooking and other Techniques for Hiding and Protection: 8
Malware Analysis System Evasion: 8
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 12
URLs 12
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 12
Public 13
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 15
Domains 15
ASN 15
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 17
Static File Info 23

General 23
File Icon 23
Static PE Info 23
General 23
Entrypoint Preview 23
Data Directories 25
Sections 25
Resources 25
Imports 25
Version Infos 26
Network Behavior 26
Network Port Distribution 26
TCP Packets 26
UDP Packets 28
DNS Queries 29
DNS Answers 29
Code Manipulations 29
Statistics 29
Behavior 30
System Behavior 30
Analysis Process: 741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe PID: 6180 Parent PID: 5616
General 3030
File Activities 30
File Created 30
File Deleted 31
File Written 31
File Read 33
Analysis Process: powershell.exe PID: 6356 Parent PID: 6180 33
General 33
File Activities 33
File Created 33
File Deleted 34
File Written 34
File Read 38
Analysis Process: conhost.exe PID: 6372 Parent PID: 6356 41
General 41
Analysis Process: schtasks.exe PID: 6412 Parent PID: 6180 41
General 41
File Activities 41
File Read 41
Analysis Process: conhost.exe PID: 6472 Parent PID: 6412 41
General 42
Analysis Process: powershell.exe PID: 6528 Parent PID: 6180 42
General 42
File Activities 42
File Created 42
File Deleted 42
File Written 43
File Read 46
Analysis Process: conhost.exe PID: 6548 Parent PID: 6528 49
General 49
Analysis Process: RegSvcs.exe PID: 6556 Parent PID: 6180 49
General 49
Analysis Process: schtasks.exe PID: 6696 Parent PID: 6556 50
General 50
Analysis Process: conhost.exe PID: 6704 Parent PID: 6696 50
General 50
Analysis Process: schtasks.exe PID: 6756 Parent PID: 6556 51
General 51
Analysis Process: conhost.exe PID: 6764 Parent PID: 6756 51
General 51
Analysis Process: RegSvcs.exe PID: 6856 Parent PID: 904 51
General 51
Analysis Process: conhost.exe PID: 6864 Parent PID: 6856 51
General 51
Analysis Process: dhcpmon.exe PID: 6872 Parent PID: 904 52
General 52
Analysis Process: conhost.exe PID: 6884 Parent PID: 6872 52
General 52
Analysis Process: dhcpmon.exe PID: 5732 Parent PID: 3472 52

General 52
Analysis Process: conhost.exe PID: 5928 Parent PID: 5732 53
General 53
Disassembly 53
Code Analysis 53

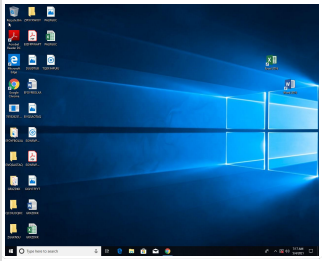
Analysis Report 741B26251FA1FBA9C4D5EB7AACA544…

Overview

General Information

Sample Name:	741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe
Analysis ID:	403532
MD5:	cdda16bd52c7c6..
SHA1:	5789cb8b8b1493..
SHA256:	741b26251fa1fba..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

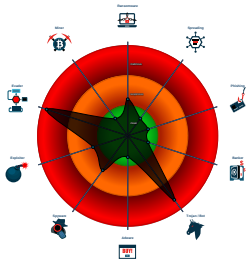
Nanocore

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

Signatures

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

Classification



Startup

- **System is w10x64**
- 741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe (PID: 6180 cmdline: 'C:\Users\user\Desktop\741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe' MD5: CDDA16BD52C7C602B534593BE9149A42)
  - powershell.exe (PID: 6356 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6372 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6412 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\gKpxRZsP' /XML 'C:\Users\user\AppData\Local\Temp\tmp30C2.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6528 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\gKpxRZsP.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6556 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 71369277D09DA0830C8C59F9E22BB23A)
    - schtasks.exe (PID: 6696 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpB146.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6704 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6756 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpB52F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6764 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 6856 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0 MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 6864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6872 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 6884 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 5732 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 5928 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "caa6fa7a-f28b-4f9f-9a4a-ce9e5290",
  "Group": "ONEZERO",
  "Domain1": "strongodss.ddns.net",
  "Domain2": "79.134.225.40",
  "Port": 48154,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8009,
  "BufferSize": "02000100",
  "MaxPacketSize": "",
  "GCThreshold": "",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.511998017.000000000434C000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000008.00000002.511998017.000000000434C000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x13a95:$a: NanoCore • 0x13aee:$a: NanoCore • 0x13b2b:$a: NanoCore • 0x13ba4:$a: NanoCore • 0x19139:$a: NanoCore • 0x19183:$a: NanoCore • 0x1936d:$a: NanoCore • 0x2cc8c:$a: NanoCore • 0x2cca1:$a: NanoCore • 0x2ccd6:$a: NanoCore • 0x45c2b:$a: NanoCore • 0x45c40:$a: NanoCore • 0x45c75:$a: NanoCore • 0x13af7:$b: ClientPlugin • 0x13b34:$b: ClientPlugin • 0x14432:$b: ClientPlugin • 0x1443f:$b: ClientPlugin • 0x18ed2:$b: ClientPlugin • 0x19142:$b: ClientPlugin • 0x1918c:$b: ClientPlugin • 0x2ca48:$b: ClientPlugin
00000000.00000002.244648700.000000000336A000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000008.00000002.513739140.000000000603000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1646:$x1: NanoCore.ClientPluginHost
00000008.00000002.513739140.000000000603000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1646:$x2: NanoCore.ClientPluginHost • 0x1724:$s4: PipeCreated • 0x1660:$s5: IClientLoggingHost
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.RegSvcs.exe.435ecb6.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0x6483:$x1: NanoCore.ClientPluginHost • 0x1a020:$x1: NanoCore.ClientPluginHost • 0x32fbf:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost • 0x1a04d:$x2: IClientNetworkHost • 0x32fec:$x2: IClientNetworkHost
8.2.RegSvcs.exe.435ecb6.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x6483:$x2: NanoCore.ClientPluginHost • 0x1a020:$x2: NanoCore.ClientPluginHost • 0x32fbf:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0x6561:$s4: PipeCreated • 0x1b0fb:$s4: PipeCreated • 0x3409a:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost • 0x649d:$s5: IClientLoggingHost • 0x1a03a:$s5: IClientLoggingHost • 0x32fd9:$s5: IClientLoggingHost
8.2.RegSvcs.exe.435ecb6.3.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
8.2.RegSvcs.exe.435ecb6.3.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xddf:$a: NanoCore • 0xe38:$a: NanoCore • 0xe75:$a: NanoCore • 0xeee:$a: NanoCore • 0x6483:$a: NanoCore • 0x64cd:$a: NanoCore • 0x66b7:$a: NanoCore • 0x19fd6:$a: NanoCore • 0x19feb:$a: NanoCore • 0x1a020:$a: NanoCore • 0x32f75:$a: NanoCore • 0x32f8a:$a: NanoCore • 0x32fbf:$a: NanoCore • 0xe41:$b: ClientPlugin • 0xe7e:$b: ClientPlugin • 0x177c:$b: ClientPlugin • 0x1789:$b: ClientPlugin • 0x621c:$b: ClientPlugin • 0x648c:$b: ClientPlugin • 0x64d6:$b: ClientPlugin • 0x19d92:$b: ClientPlugin
8.2.RegSvcs.exe.3321364.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x40c2:$x1: NanoCore.ClientPluginHost
Click to see the 42 entries				

Sigma Overview

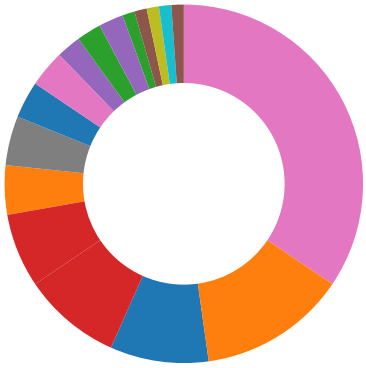
System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview

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



Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for domain / URL
- 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)

Data Obfuscation:

- .NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

- Yara detected AntiVM3

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

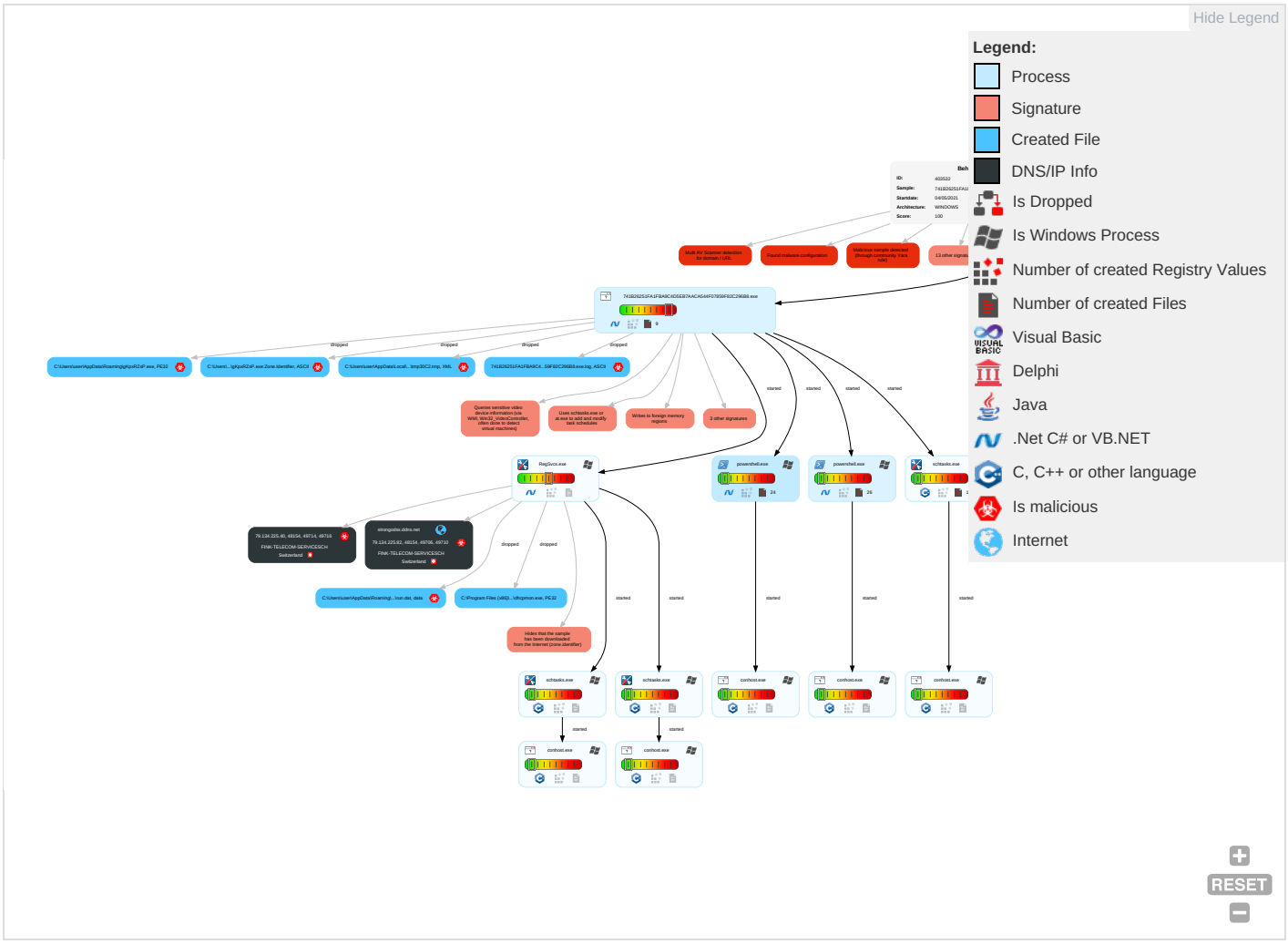
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1 1	Input Capture 2 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 3	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 2	NTDS	Security Software Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 3 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

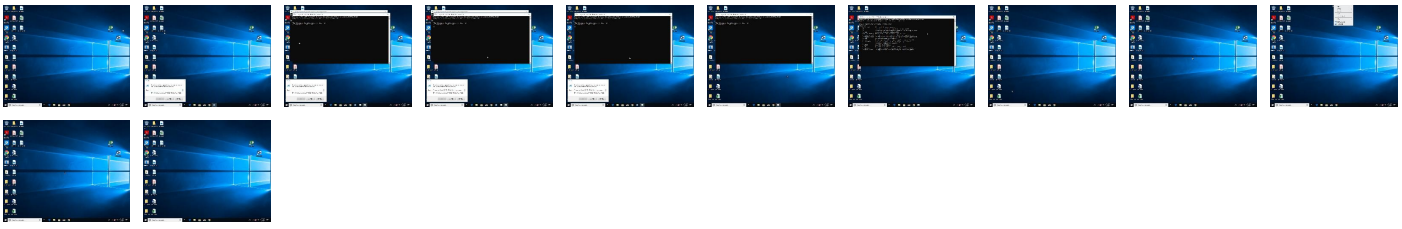
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe	59%	Virustotal		Browse
741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe	24%	Metadefender		Browse
741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe	72%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\gKpxRZsP.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\gKpxRZsP.exe	24%	Metadefender		Browse
C:\Users\user\AppData\Roaming\gKpxRZsP.exe	72%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.RegSvcs.exe.6040000.10.unpack	100%	Avira	TR/NanoCore.fadte		Download File
8.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
79.134.225.40	7%	Virustotal		Browse
79.134.225.40	0%	Avira URL Cloud	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	
strongodss.ddns.net	8%	Virustotal		Browse
strongodss.ddns.net	0%	Avira URL Cloud	safe	
http://crl.mi	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
strongodss.ddns.net	79.134.225.82	true	true	• 8%, Virustotal, Browse	unknown

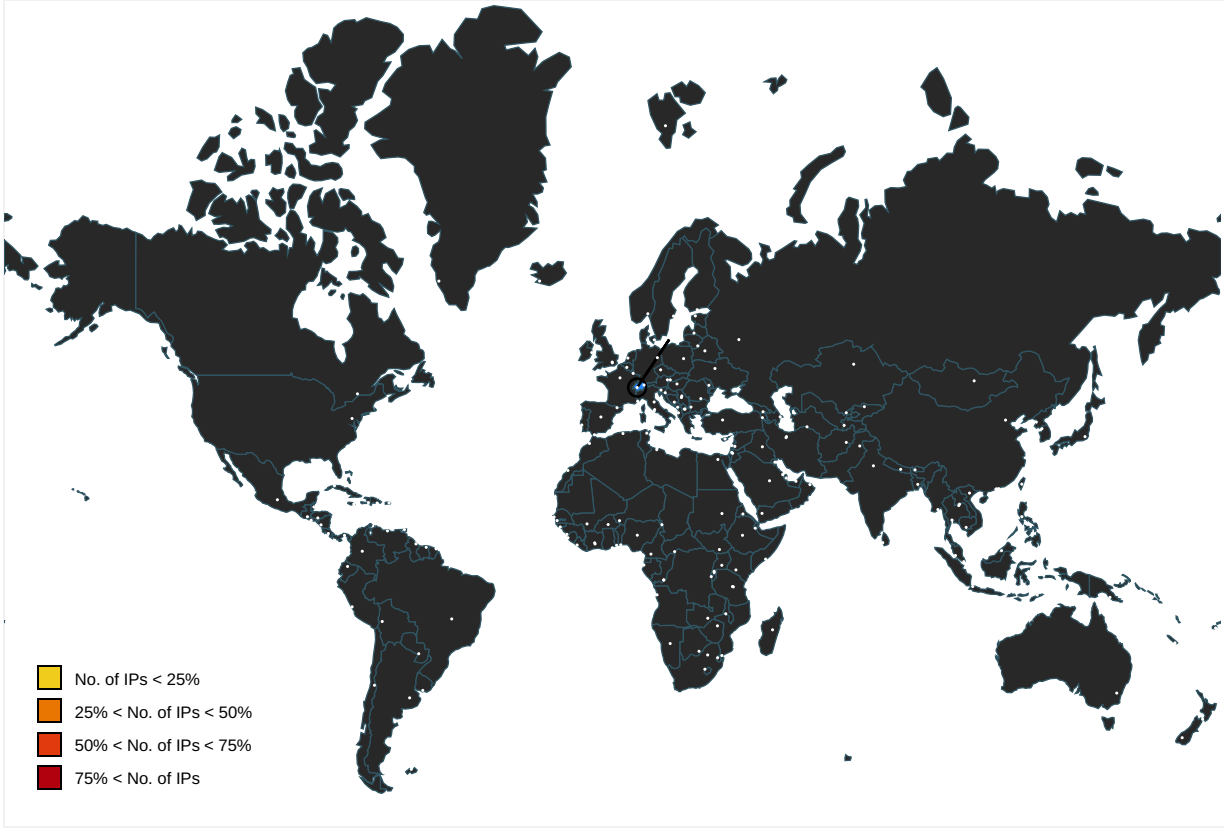
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
79.134.225.40	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
strongodss.ddns.net	true	• 8%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://go.micro	powershell.exe, 00000002.00000003.318477069.0000000005695000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe, 00000000.00000002.244648700.000000000336A000.00000004.00000001.sdmp	false		high
http://crl.mi	powershell.exe, 00000006.00000003.352217202.0000000009532000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.40	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true
79.134.225.82	strongodss.ddns.net	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403532
Start date:	04.05.2021
Start time:	07:14:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.evad.winEXE@24/24@9/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.1% (good quality ratio 0.8%) • Quality average: 41.5% • Quality standard deviation: 35.4%
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. • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 93.184.220.29, 20.50.102.62, 13.64.90.137, 92.122.145.129, 13.88.21.125, 92.122.145.220, 92.122.144.200, 20.82.210.154, 92.122.213.194, 92.122.213.247, 20.54.26.129 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, storeedgefd.xbetservices.akadns.net, e12564.dspb.akamaiedge.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, storeedgefd.dsx.mp.microsoft.com, www.bing.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, e16646.dscg.akamaiedge.net, skypedataprdcolwus15.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:15:31	API Interceptor	1x Sleep call for process: 741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe modified
07:15:39	API Interceptor	956x Sleep call for process: RegSvcs.exe modified
07:15:39	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
07:15:40	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe" s>$(Arg0)
07:15:40	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
07:16:04	API Interceptor	72x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.40	kYXjS6Oc3S.exe	Get hash	malicious	Browse	
	eK1KiJlz3l.exe	Get hash	malicious	Browse	
	80tzo8FG3d.exe	Get hash	malicious	Browse	
	zunUbtZ2Y3.exe	Get hash	malicious	Browse	
	cJtVGjtNGZ.exe	Get hash	malicious	Browse	
	3aDHivUqWtumbXb.exe	Get hash	malicious	Browse	
	fMy120EQiT6NaRd.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Bulz.394792.29952.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.578.18498.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.DownLoader36.32796.17922.exe	Get hash	malicious	Browse	
	HOqJcenF6O.exe	Get hash	malicious	Browse	
	0l2ddZZKv7.exe	Get hash	malicious	Browse	
	Q2BZ01fmwK.exe	Get hash	malicious	Browse	
	eO769dBnEg.exe	Get hash	malicious	Browse	
	compiled_report_2020_xls.exe	Get hash	malicious	Browse	
	all_reports_compiled_xls_2020_contact_details.exe	Get hash	malicious	Browse	
	9dAVqCPNyn.exe	Get hash	malicious	Browse	
	M5NwREJ2Yc.exe	Get hash	malicious	Browse	
	lyrvDJCi1i.exe	Get hash	malicious	Browse	
	FUyv1AeebX.exe	Get hash	malicious	Browse	
79.134.225.82	619DBBJxtN.exe	Get hash	malicious	Browse	
	EUjk8F87b8.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	DHL_SHIPPING_DOCS_INV.exe	Get hash	malicious	Browse	
	Lime_ShipDoc_PDF.exe	Get hash	malicious	Browse	
	Upgrade Form.exe	Get hash	malicious	Browse	
	Upgrade Form.exe	Get hash	malicious	Browse	
	Our Ref. 786-16-AZ-519CDN - Order.exe	Get hash	malicious	Browse	
	REN42159.jar	Get hash	malicious	Browse	
	SAMPLE_P.JAR	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
strongodss.ddns.net	kYXjS6Oc3S.exe	Get hash	malicious	Browse	• 105.112.99.190
	eK1KiJlz3l.exe	Get hash	malicious	Browse	• 105.112.99.190
	80tzo8FG3d.exe	Get hash	malicious	Browse	• 105.112.98.238
	zunUbtZ2Y3.exe	Get hash	malicious	Browse	• 79.134.225.40
	cJtVGjtNGZ.exe	Get hash	malicious	Browse	• 79.134.225.40
	3aDHivUqWtumbXb.exe	Get hash	malicious	Browse	• 105.112.99.199
	fMy120EQiT6NaRd.exe	Get hash	malicious	Browse	• 79.134.225.40
	SecuriteInfo.com.Variant.Bulz.394792.29952.exe	Get hash	malicious	Browse	• 105.112.98.171
	SecuriteInfo.com.Trojan.PackedNET.578.18498.exe	Get hash	malicious	Browse	• 105.112.98.171
	nq0aCrCXyE.exe	Get hash	malicious	Browse	• 87.237.165.78
	73SriHObnQ.exe	Get hash	malicious	Browse	• 87.237.165.78
	rb86llCYzA.exe	Get hash	malicious	Browse	• 87.237.165.78
	uB8OTxUd3O.exe	Get hash	malicious	Browse	• 87.237.165.78
	NNb2NBgsob.exe	Get hash	malicious	Browse	• 87.237.165.78
	cp573oYDUX.exe	Get hash	malicious	Browse	• 87.237.165.78
	Y5XyMnx8Ng.exe	Get hash	malicious	Browse	• 87.237.165.78
	YoWPu2BQzA9FeDd.exe	Get hash	malicious	Browse	• 87.237.165.78
	M5QDAaK9yM.exe	Get hash	malicious	Browse	• 87.237.165.78
	TdX45jQWjj.exe	Get hash	malicious	Browse	• 87.237.165.78

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	Payment Advice-BCS_ECS9522020909153934_3159_952.jar	Get hash	malicious	Browse	• 79.134.225.17
	Stub.exe	Get hash	malicious	Browse	• 79.134.225.125
	Q-B210426002.exe	Get hash	malicious	Browse	• 79.134.225.125
	Transcation23032021pdf.exe	Get hash	malicious	Browse	• 79.134.225.70
	471e3984_by_Libranalysis.docx	Get hash	malicious	Browse	• 79.134.225.26

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#KV18RE001_A5491NGOCQUANGTRADEPRODUCTIONSERVICE5.exe	Get hash	malicious	Browse	• 79.134.225.91
	b2NaDSFu9T.exe	Get hash	malicious	Browse	• 79.134.225.26
	Original title deed.xlsx	Get hash	malicious	Browse	• 79.134.225.26
	ORDER INQUIRY.doc	Get hash	malicious	Browse	• 79.134.225.52
	To1sRo1E8P.exe	Get hash	malicious	Browse	• 79.134.225.25
	BhTxt5BUvy.exe	Get hash	malicious	Browse	• 79.134.225.25
	SCAN_ORDER & SAMPLES.exe	Get hash	malicious	Browse	• 79.134.225.52
	Apr-advance payment #5972939.exe	Get hash	malicious	Browse	• 79.134.225.9
	PpkzTxJVyC.exe	Get hash	malicious	Browse	• 79.134.225.26
	Original title deed.xlsx	Get hash	malicious	Browse	• 79.134.225.26
	swift copy.exe	Get hash	malicious	Browse	• 79.134.225.48
	swift copy.exe	Get hash	malicious	Browse	• 79.134.225.48
	jk55xlWn7a.exe	Get hash	malicious	Browse	• 79.134.225.26
	Qds5xiJaAX.exe	Get hash	malicious	Browse	• 79.134.225.26
	INVOICE.xlsx	Get hash	malicious	Browse	• 79.134.225.26
FINK-TELECOM-SERVICESCH	Payment Advice-BCS_ECS9522020909153934_3159_952.jar	Get hash	malicious	Browse	• 79.134.225.17
	Stub.exe	Get hash	malicious	Browse	• 79.134.225.125
	Q-B210426002.exe	Get hash	malicious	Browse	• 79.134.225.125
	Transcation23032021pdf.exe	Get hash	malicious	Browse	• 79.134.225.70
	471e3984_by_Libranalysis.docx	Get hash	malicious	Browse	• 79.134.225.26
	PO#KV18RE001_A5491NGOCQUANGTRADEPRODUCTIONSERVICE5.exe	Get hash	malicious	Browse	• 79.134.225.91
	b2NaDSFu9T.exe	Get hash	malicious	Browse	• 79.134.225.26
	Original title deed.xlsx	Get hash	malicious	Browse	• 79.134.225.26
	ORDER INQUIRY.doc	Get hash	malicious	Browse	• 79.134.225.52
	To1sRo1E8P.exe	Get hash	malicious	Browse	• 79.134.225.25
	BhTxt5BUvy.exe	Get hash	malicious	Browse	• 79.134.225.25
	SCAN_ORDER & SAMPLES.exe	Get hash	malicious	Browse	• 79.134.225.52
	Apr-advance payment #5972939.exe	Get hash	malicious	Browse	• 79.134.225.9
	PpkzTxJVyC.exe	Get hash	malicious	Browse	• 79.134.225.26
	Original title deed.xlsx	Get hash	malicious	Browse	• 79.134.225.26
	swift copy.exe	Get hash	malicious	Browse	• 79.134.225.48
	swift copy.exe	Get hash	malicious	Browse	• 79.134.225.48
	jk55xlWn7a.exe	Get hash	malicious	Browse	• 79.134.225.26
	Qds5xiJaAX.exe	Get hash	malicious	Browse	• 79.134.225.26
	INVOICE.xlsx	Get hash	malicious	Browse	• 79.134.225.26

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Doc.17135273873.5A0AFF5F.exe	Get hash	malicious	Browse	
	eReceipt.pdf.exe	Get hash	malicious	Browse	
	TPA AGREEMENT00038499530.exe	Get hash	malicious	Browse	
	Swift copy.exe	Get hash	malicious	Browse	
	f90FtWrVT4.exe	Get hash	malicious	Browse	
	kYXjS6Oc3S.exe	Get hash	malicious	Browse	
	eK1KiJlz3l.exe	Get hash	malicious	Browse	
	80tzo8FG3d.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.645.23105.exe	Get hash	malicious	Browse	
	JQEl8bosea.exe	Get hash	malicious	Browse	
	YfceI5MZX4.exe	Get hash	malicious	Browse	
	TSskTqG9V9.exe	Get hash	malicious	Browse	
	oE6O5K1emC.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	wDlaJji4Vv.exe	Get hash	malicious	Browse	
	cJtVGjtNGZ.exe	Get hash	malicious	Browse	
	Bilansno placanje.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Inject4.9647.20479.exe	Get hash	malicious	Browse	
	wnIPBdB5OF.exe	Get hash	malicious	Browse	
	Delivery Form C.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.7515815714465193
Encrypted:	false
SSDEEP:	384:BOj9Y8/gS7SDriLGKq1MHR5U4Ag6ihJSxUCR1rgCPKabK2t0X5P7DZ+JgWSW72uw:B+gSAdN1MH3HAFRJngW2u
MD5:	71369277D09DA0830C8C59F9E22BB23A
SHA1:	37F9781314F0F6B7E9CB529A573F2B1C8DE9E93F
SHA-256:	D4527B7AD2FC4778CC5BE8709C95AEA44EAC0568B367EE14F7357D72898C3698
SHA-512:	2F470383E3C796C4CF212EC280854DBB9E7E8C8010CE6857E58F8E7066D7516B7CD7039BC5C0F547E1F5C7F9F2287869ADFFB2869800B08B2982A88BE96E9FB7
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Doc.17135273873.5A0AFF5F.exe, Detection: malicious, Browse • Filename: eReceipt.pdf.exe, Detection: malicious, Browse • Filename: TPA AGREEMENT00038499530.exe, Detection: malicious, Browse • Filename: Swift copy.exe, Detection: malicious, Browse • Filename: f90FtWrVT4.exe, Detection: malicious, Browse • Filename: kYXjS6Oc3S.exe, Detection: malicious, Browse • Filename: eK1KiJlz3l.exe, Detection: malicious, Browse • Filename: 80tzo8FG3d.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.645.23105.exe, Detection: malicious, Browse • Filename: JQEl8bosea.exe, Detection: malicious, Browse • Filename: YfceI5MZX4.exe, Detection: malicious, Browse • Filename: TSskTqG9V9.exe, Detection: malicious, Browse • Filename: oE6O5K1emC.exe, Detection: malicious, Browse • Filename: GS_ PO NO.1862021.exe, Detection: malicious, Browse • Filename: wDIaJji4Vv.exe, Detection: malicious, Browse • Filename: cJtVGjtNGZ.exe, Detection: malicious, Browse • Filename: Bilansno placanje.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Inject4.9647.20479.exe, Detection: malicious, Browse • Filename: wnIPBdB5OF.exe, Detection: malicious, Browse • Filename: Delivery Form C.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{Z.....P... .....k.. .....@.. .....[.. ..@.....k..K..... k..... ....H.....text....K... ...P..... ..`.rsrc.....`.....@..@.rel oc.....p.....@..B.....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe.log	
Process:	C:\Users\user\Desktop\741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1046
Entropy (8bit):	5.270787694394625
Encrypted:	false
SSDEEP:	24:MLF20NaL3z2p29hJ5g522rW2xAi3AP26K95rKoO2+g2s29XBT:MwLLD2Y9h3go2rxxAcAO6ox+g2X9XBT
MD5:	ED4EBBF50955129F980394522E6F689E
SHA1:	4DFA7FEDB46CD096E5869EFFC8FB74FE333B295A
SHA-256:	B8ED8F33F5E6A5DA8ACE56720245C651D63ED0C7415B640B33445425284490EE
SHA-512:	2611B22AE6D0DF50BEC60A1817FBB01AE754534BBDDB4BAA7F8171C256F2883837CDB3475E3B1E8B9D1B59D04C0496EB951486D355B352E6F266124117C0AD9
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages _v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Wind ows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\3577 4dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\de460308a909923 7864d2ec2328fc958\System.Configuration.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System .Xml.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management\4de99804c29261ed

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegSvcs.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegSvcs.exe.log	
Entropy (8bit):	5.016405576253028
Encrypted:	false
SSDEEP:	3:QHXMKaoWglAFXMWA2yTMGfsbNXLVd49Am12MFuAvOAsDeieVyn:Q3LawlAFXMWTyAGCFLIP12MUAvvrs
MD5:	50DEC1858E13F033E6DCA3CBFAD5E8DE
SHA1:	79AE1E9131B0FAF215B499D2F7B4C595AA120925
SHA-256:	14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4
SHA-512:	1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF
Malicious:	false
Preview:	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

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

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-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\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22328
Entropy (8bit):	5.601278954858116
Encrypted:	false
SSDEEP:	384:btCDP00mgs1KuTOYSBKnWsIiD7Y9ghSJUeRu1BMrmrZ1AVlcer564I+Bzg:9gmB4KWsd3hXe1a43U
MD5:	99031A08329636158D3AEF935E655921
SHA1:	E3B6128B5A081B87303D9A16BBC4BE9B2C63363C
SHA-256:	CA726B47B1B806EDC010F4DB35D8BDB1C1D75548634A8B53E1C698819E6321A7
SHA-512:	72838EF3ED6F7BDE35D08E906D7341C09529407F48DE7F7F53800706272D97B9EFF9F65DCB6577910B10055250BD6F22BBA6F21240C1EB344CE0C677088B1677
Malicious:	false
Preview:	@...e.....u.t.d.D.....4.....@.....H.....<@.^.L."My...:R..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....//.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_eywfmlgy.1th.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gof3hya4.2ip.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_y2xejyx0.1ov.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_y5ptkebd.tnb.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp\tmp30C2.tmp	
Process:	C:\Users\user\Desktop\741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.170042432643481
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBatn:cbhC7ZlNQF/rydbz9I3YODOLNdq3+
MD5:	32319A48FC91674BB574177853C94741
SHA1:	63293D27D77CD683D60199A2D61FF76EDAC36584
SHA-256:	03350CAC52945A5551E07DA2647F400D39DF30B849A00FFBE60B466CC704B77D
SHA-512:	0B29A67F9B376AE3AADCC83B3B2B381C571330BA63B0104819A9B0DFF65DA3019454826AF9A5CDDD249C031D938D52143BA6EE33FC40F615EF00979BDE4D31E2
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Local\Temp\tmpB146.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.135021273392143
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mn4xtn:cbk4oL600QydbQxIYODOLedq3Z4j
MD5:	40B11EF601FB28F9B2E69D36857BF2EC
SHA1:	B6454020AD2CEED193F4792B77001D0BD741B370
SHA-256:	C51E12D18CC664425F6711D8AE2507068884C7057092CFA11884100E1E9D49E1
SHA-512:	E3C5BCC714CBFCA4B8058DDCDDF231DCEFA69C15881CE3F8123E59ED45CFB5DA052B56E1945DCF8DC7F800D62F9A4EECB82BCA69A66A1530787AEFFEB15E2BD5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpB52F.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:pTN:FN
MD5:	411EF39A6DB99EE949EEA4ACEA7229D3
SHA1:	C9B3F9D84DE0D440557D2B095AF10BE38CC2346E
SHA-256:	16FC08F263A59F50DB07FBA479137CDE9D872C3CB0E1A08095D2464DBB39F58E
SHA-512:	FCAD00F3AD8AFC28DD7B273DF192644A2D6E95A517D56EBDBF0E2A670027A3294608E8A42777504B752C2EC420806A13E7086F8DD06489690CC0EEED2C5785A
Malicious:	**true**
Preview:	.......H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.795707286467131
Encrypted:	false
SSDEEP:	3:oMty8WbSX/MNn:oMLWus
MD5:	D685103573539B7E9FDBF5F1D7DD96CE
SHA1:	4B2FE6B5C0B37954B314FCAEE1F12237A9B02D07
SHA-256:	D78BC23B0CA3EDDF52D56AB85CDC30A71B3756569CB32AA2F6C28DBC23C76E8E
SHA-512:	17769A5944E8929323A34269ABEEF0861D5C6799B0A27F5545FBFADC80E5AB684A471AD6F6A7FC623002385154EA89DE94013051E09120AB94362E542AB0F1DD
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe

C:\Users\user\AppData\Roaming\gKpxRZsP.exe	
Process:	C:\Users\user\Desktop\741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	786944
Entropy (8bit):	7.1725977137745875
Encrypted:	false
SSDEEP:	12288:r5miJJsGELK+yZRK1Wc++qRz/C3TfpCMsv0nSCB0eXfw1AgZaWm:nELKNRK1Wnr4wPCB0YfH
MD5:	CDDA16BD52C7C602B534593BE9149A42
SHA1:	5789CB8B8B1493DE3733C66CD52D8B0180BE6CD4
SHA-256:	741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8C01D2339A4EA2D06C58
SHA-512:	680E5DAA2A32D5C6AE39A15B5EB0F486C1805DC9DC4B4CACBB7B7B53C658F398B00C5D1EF0FD536E4475A7ABC72CEB11F79CDEBDF600D2D6B9A9DAEC674B4A60
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 24%, Browse • Antivirus: ReversingLabs, Detection: 72%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...N:_`.....R.... ... ....@.. .....`..... ..@.....W....@..4..... ....H.....text...X.... ....`.reloc..... .....@..B.rsr c...4....@.....@..@.....4.....H.....T-.....p4.....z.(.....}.....(...o!...}....*..*...0.....{.....E.....8...Z...u.....*..}.....].4S }.....}.....*..}..... ..Q.}.....}.....*..}.....{.... Km.a}.....}.....*..}..... ,...}.....}.....*..}.....{.... ..=.a}.....}.....*..}..... ....}.....}.....*..}..... "G.R}.....}.....*..}.....*...{....*.s"...z.2.{.....*....0..<..... {.....3..{....(...o!...3...}.....+..s.....{....}..

C:\Users\user\AppData\Roaming\gKpxRZsP.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**

C:\Users\user\AppData\Roaming\gKpxRZsP.exe:Zone.Identifier	
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210504\PowerShell_transcript.813435.K7iDO9IF.20210504071538.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):	5791
Entropy (8bit):	5.392694650450653
Encrypted:	false
SSDEEP:	96:BZM/SNSqDo1Z4Zj/SNSqDo1Z3bFjjZD/SNSqDo1ZNmTTzZo:N
MD5:	6331AE1D412EBC7310F52FEB97831F58
SHA1:	8690725843D19FAD0528F7B9F4CA596C3D6C6D9A
SHA-256:	EE9DBA77E8DB16DB13D081C3222B75F76FCD90701F03F57860CFE8849D02EE31
SHA-512:	5859EE84DDC687E5E349FEE6CFD69477385CCD8025A5339F67D04F2F9CECF608399B02E3B5F3110BB0CEC59C8252F57C800DDF070E44561F6B3718B83F89ADE
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210504071558..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 813435 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\gKpxRZsP.exe..Process ID: 6528..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: 20210504071559..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\gKpxRZsP.exe..**********..Windows PowerShell transcript start..Start time: 20210504072121..Username: computer\user..RunAs User: computer\alf

C:\Users\user\Documents\20210504\PowerShell_transcript.813435.WJkwONF7.20210504071534.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):	5907
Entropy (8bit):	5.441485082708644
Encrypted:	false
SSDEEP:	96:BZQ/SN0cIqDo1ZIc5ZP/SN0cIqDo1Z54u+uQujZC/SN0cIqDo1Zo5uAuAuNZ2:JQkQH
MD5:	D88A09D4A60F78F280D1CAEDB6511E46
SHA1:	32E5507909FFA40EB273EC0009FD441DE1062DAB
SHA-256:	F86EDDD54173F82E09383DCB45FECB80ACEFDB5F0A46C066F65CA189B862C795
SHA-512:	A8B3749C63B0B53C0AB8C390EF5BD886FE32355765E7978001CB00822A1D0A3EA7664D16B81999EA57A52EADE9EDC6AAB40576FF1C4EEF772029BBE190BB753 5
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210504071554..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 813435 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe..Process ID: 6356..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: 20210504071555..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe..**********..Windows PowerShell transcript start..Start time: 20210504071854..Usernam

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1145
Entropy (8bit):	4.462201512373672
Encrypted:	false
SSDEEP:	24:zKLXkzPDObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0zPDQntKKH1MqJC
MD5:	46EBEB88876A00A52CC37B1F8E0D0438
SHA1:	5E5DB352F964E5F398301662FF558BD905798A65
SHA-256:	D65BD5A6CC112838AFE8FA70BF61FD13C1313BCE3EE3E76C50E454D7B581238B
SHA-512:	E713E6F304A469FB71235C598BC7E2C6F8458ABC61DAF3D1F364F66579CAFA4A7F3023E585BDA552FB400009E7805A8CA0311A50D5EDC9C2AD2D067772A071E E
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Reconfigure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo Suppress logo output... /quiet Suppress logo output and success output...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.1725977137745875
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe
File size:	786944
MD5:	cdda16bd52c7c602b534593be9149a42
SHA1:	5789cb8b8b1493de3733c66cd52d8b0180be6cd4
SHA256:	741b26251fa1fba9c4d5eb7aaca544f07859f82c296b8c01d2339a4ea2d06c58
SHA512:	680e5daa2a32d5c6ae39a15b5eb0f486c1805dc9dc4b4cacbb7b7b53c658f398b00c5d1ef0fd536e4475a7abc72ceb11f79cdebdf600d2d6b9a9daec674b4a60
SSDEEP:	12288:r5miJJsGELK+yZRK1Wc++qRz/C3TfpCMsv0nSCB0eXfw1AgZaWm:nELKNRK1Wnr4wPCB0YfH
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...N:_`.....R.... ... ....@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c1652
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x605F3A4E [Sat Mar 27 13:59:42 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc15f8	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc4000	0x434	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc2000	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	0xbf658	0xbf800	False	0.640252733355	data	7.17998377305	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0xc2000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0xc4000	0x434	0x600	False	0.284505208333	data	2.45393022551	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc4058	0x3dc	data		

Imports

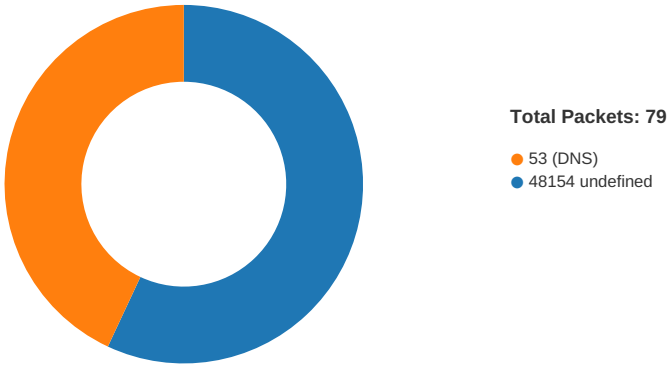
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright The Ridgeway School 2014
Assembly Version	1.0.0.0
InternalName	SoapYearMonth.exe
FileVersion	1.0.0.0
CompanyName	The Ridgeway School & Sixth Form College
LegalTrademarks	
Comments	
ProductName	Ridgeway Cover Manager
ProductVersion	1.0.0.0
FileDescription	Ridgeway Cover Manager
OriginalFilename	SoapYearMonth.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 07:15:27.042237997 CEST	49706	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:15:27.273075104 CEST	48154	49706	79.134.225.82	192.168.2.5
May 4, 2021 07:15:27.885104895 CEST	49706	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:15:28.122991085 CEST	48154	49706	79.134.225.82	192.168.2.5
May 4, 2021 07:15:28.696151018 CEST	49706	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:15:45.586889982 CEST	49710	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:15:45.816423893 CEST	48154	49710	79.134.225.82	192.168.2.5
May 4, 2021 07:15:46.488142014 CEST	49710	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:15:46.727307081 CEST	48154	49710	79.134.225.82	192.168.2.5
May 4, 2021 07:15:47.300519943 CEST	49710	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:16:03.492914915 CEST	49713	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:16:06.567784071 CEST	49713	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:16:06.799026012 CEST	48154	49713	79.134.225.82	192.168.2.5
May 4, 2021 07:16:07.380307913 CEST	49713	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:16:07.610522032 CEST	48154	49713	79.134.225.82	192.168.2.5
May 4, 2021 07:16:11.936126947 CEST	49714	48154	192.168.2.5	79.134.225.40
May 4, 2021 07:16:12.012255907 CEST	48154	49714	79.134.225.40	192.168.2.5
May 4, 2021 07:16:12.630789995 CEST	49714	48154	192.168.2.5	79.134.225.40
May 4, 2021 07:16:12.707016945 CEST	48154	49714	79.134.225.40	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 07:16:13.214102030 CEST	49714	48154	192.168.2.5	79.134.225.40
May 4, 2021 07:16:13.290311098 CEST	48154	49714	79.134.225.40	192.168.2.5
May 4, 2021 07:16:17.305704117 CEST	49716	48154	192.168.2.5	79.134.225.40
May 4, 2021 07:16:17.381788015 CEST	48154	49716	79.134.225.40	192.168.2.5
May 4, 2021 07:16:17.881215096 CEST	49716	48154	192.168.2.5	79.134.225.40
May 4, 2021 07:16:17.958976984 CEST	48154	49716	79.134.225.40	192.168.2.5
May 4, 2021 07:16:18.459405899 CEST	49716	48154	192.168.2.5	79.134.225.40
May 4, 2021 07:16:18.535582066 CEST	48154	49716	79.134.225.40	192.168.2.5
May 4, 2021 07:16:22.540847063 CEST	49717	48154	192.168.2.5	79.134.225.40
May 4, 2021 07:16:22.616911888 CEST	48154	49717	79.134.225.40	192.168.2.5
May 4, 2021 07:16:23.131656885 CEST	49717	48154	192.168.2.5	79.134.225.40
May 4, 2021 07:16:23.207626104 CEST	48154	49717	79.134.225.40	192.168.2.5
May 4, 2021 07:16:23.709866047 CEST	49717	48154	192.168.2.5	79.134.225.40
May 4, 2021 07:16:23.786063910 CEST	48154	49717	79.134.225.40	192.168.2.5
May 4, 2021 07:16:27.884485960 CEST	49718	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:16:30.898025036 CEST	49718	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:16:31.154237986 CEST	48154	49718	79.134.225.82	192.168.2.5
May 4, 2021 07:16:31.663722038 CEST	49718	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:16:31.910223961 CEST	48154	49718	79.134.225.82	192.168.2.5
May 4, 2021 07:16:36.085549116 CEST	49719	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:16:36.365506887 CEST	48154	49719	79.134.225.82	192.168.2.5
May 4, 2021 07:16:36.867202997 CEST	49719	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:16:37.116184950 CEST	48154	49719	79.134.225.82	192.168.2.5
May 4, 2021 07:16:37.617296934 CEST	49719	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:16:37.851423979 CEST	48154	49719	79.134.225.82	192.168.2.5
May 4, 2021 07:16:41.986804008 CEST	49720	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:16:42.222215891 CEST	48154	49720	79.134.225.82	192.168.2.5
May 4, 2021 07:16:42.727555037 CEST	49720	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:16:48.743103981 CEST	49720	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:16:49.019256115 CEST	48154	49720	79.134.225.82	192.168.2.5
May 4, 2021 07:16:53.027044058 CEST	49725	48154	192.168.2.5	79.134.225.40
May 4, 2021 07:16:53.103339911 CEST	48154	49725	79.134.225.40	192.168.2.5
May 4, 2021 07:16:53.688102007 CEST	49725	48154	192.168.2.5	79.134.225.40
May 4, 2021 07:16:53.768922091 CEST	48154	49725	79.134.225.40	192.168.2.5
May 4, 2021 07:16:54.337349892 CEST	49725	48154	192.168.2.5	79.134.225.40
May 4, 2021 07:16:54.415210009 CEST	48154	49725	79.134.225.40	192.168.2.5
May 4, 2021 07:16:58.432674885 CEST	49726	48154	192.168.2.5	79.134.225.40
May 4, 2021 07:16:58.508970976 CEST	48154	49726	79.134.225.40	192.168.2.5
May 4, 2021 07:16:59.009691954 CEST	49726	48154	192.168.2.5	79.134.225.40
May 4, 2021 07:16:59.088284969 CEST	48154	49726	79.134.225.40	192.168.2.5
May 4, 2021 07:16:59.603517056 CEST	49726	48154	192.168.2.5	79.134.225.40
May 4, 2021 07:16:59.679639101 CEST	48154	49726	79.134.225.40	192.168.2.5
May 4, 2021 07:17:03.698977947 CEST	49727	48154	192.168.2.5	79.134.225.40
May 4, 2021 07:17:03.775233030 CEST	48154	49727	79.134.225.40	192.168.2.5
May 4, 2021 07:17:04.291471004 CEST	49727	48154	192.168.2.5	79.134.225.40
May 4, 2021 07:17:04.367512941 CEST	48154	49727	79.134.225.40	192.168.2.5
May 4, 2021 07:17:04.869575024 CEST	49727	48154	192.168.2.5	79.134.225.40
May 4, 2021 07:17:04.945739985 CEST	48154	49727	79.134.225.40	192.168.2.5
May 4, 2021 07:17:09.076580048 CEST	49728	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:17:09.313380957 CEST	48154	49728	79.134.225.82	192.168.2.5
May 4, 2021 07:17:09.822989941 CEST	49728	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:17:10.055103064 CEST	48154	49728	79.134.225.82	192.168.2.5
May 4, 2021 07:17:10.557512999 CEST	49728	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:17:10.789951086 CEST	48154	49728	79.134.225.82	192.168.2.5
May 4, 2021 07:17:14.967493057 CEST	49730	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:17:15.222265005 CEST	48154	49730	79.134.225.82	192.168.2.5
May 4, 2021 07:17:15.729829073 CEST	49730	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:17:15.968373060 CEST	48154	49730	79.134.225.82	192.168.2.5
May 4, 2021 07:17:16.479758978 CEST	49730	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:17:16.713480949 CEST	48154	49730	79.134.225.82	192.168.2.5
May 4, 2021 07:17:20.835736036 CEST	49731	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:17:21.096276999 CEST	48154	49731	79.134.225.82	192.168.2.5
May 4, 2021 07:17:21.605381012 CEST	49731	48154	192.168.2.5	79.134.225.82
May 4, 2021 07:17:27.606126070 CEST	49731	48154	192.168.2.5	79.134.225.82

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 07:17:27.841981888 CEST	48154	49731	79.134.225.82	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 07:15:06.653614044 CEST	52704	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:06.703430891 CEST	53	52704	8.8.8.8	192.168.2.5
May 4, 2021 07:15:06.820470095 CEST	52212	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:06.865787029 CEST	54302	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:06.869576931 CEST	53	52212	8.8.8.8	192.168.2.5
May 4, 2021 07:15:06.925875902 CEST	53	54302	8.8.8.8	192.168.2.5
May 4, 2021 07:15:07.679445028 CEST	53784	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:07.728008032 CEST	53	53784	8.8.8.8	192.168.2.5
May 4, 2021 07:15:08.577774048 CEST	65307	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:08.626523972 CEST	53	65307	8.8.8.8	192.168.2.5
May 4, 2021 07:15:09.312494040 CEST	64344	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:09.371244907 CEST	53	64344	8.8.8.8	192.168.2.5
May 4, 2021 07:15:09.795833111 CEST	62060	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:09.844664097 CEST	53	62060	8.8.8.8	192.168.2.5
May 4, 2021 07:15:11.172401905 CEST	61805	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:11.226651907 CEST	53	61805	8.8.8.8	192.168.2.5
May 4, 2021 07:15:12.382261038 CEST	54795	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:12.432383060 CEST	53	54795	8.8.8.8	192.168.2.5
May 4, 2021 07:15:13.655855894 CEST	49557	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:13.712975979 CEST	53	49557	8.8.8.8	192.168.2.5
May 4, 2021 07:15:15.134202957 CEST	61733	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:15.185801029 CEST	53	61733	8.8.8.8	192.168.2.5
May 4, 2021 07:15:16.362359047 CEST	65447	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:16.422347069 CEST	53	65447	8.8.8.8	192.168.2.5
May 4, 2021 07:15:16.935184002 CEST	52441	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:16.996756077 CEST	53	52441	8.8.8.8	192.168.2.5
May 4, 2021 07:15:19.004904032 CEST	62176	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:19.057884932 CEST	53	62176	8.8.8.8	192.168.2.5
May 4, 2021 07:15:20.467269897 CEST	59596	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:20.515886068 CEST	53	59596	8.8.8.8	192.168.2.5
May 4, 2021 07:15:22.522505045 CEST	65296	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:22.574302912 CEST	53	65296	8.8.8.8	192.168.2.5
May 4, 2021 07:15:24.074537992 CEST	63183	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:24.123266935 CEST	53	63183	8.8.8.8	192.168.2.5
May 4, 2021 07:15:26.659554005 CEST	60151	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:26.716960907 CEST	53	60151	8.8.8.8	192.168.2.5
May 4, 2021 07:15:32.578547001 CEST	56969	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:32.643374920 CEST	53	56969	8.8.8.8	192.168.2.5
May 4, 2021 07:15:45.498770952 CEST	55161	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:45.557560921 CEST	53	55161	8.8.8.8	192.168.2.5
May 4, 2021 07:15:49.068558931 CEST	54757	53	192.168.2.5	8.8.8.8
May 4, 2021 07:15:49.120039940 CEST	53	54757	8.8.8.8	192.168.2.5
May 4, 2021 07:16:03.390650034 CEST	49992	53	192.168.2.5	8.8.8.8
May 4, 2021 07:16:03.449012995 CEST	53	49992	8.8.8.8	192.168.2.5
May 4, 2021 07:16:13.110769033 CEST	60075	53	192.168.2.5	8.8.8.8
May 4, 2021 07:16:13.170929909 CEST	53	60075	8.8.8.8	192.168.2.5
May 4, 2021 07:16:27.824098110 CEST	55016	53	192.168.2.5	8.8.8.8
May 4, 2021 07:16:27.882668018 CEST	53	55016	8.8.8.8	192.168.2.5
May 4, 2021 07:16:36.024789095 CEST	64345	53	192.168.2.5	8.8.8.8
May 4, 2021 07:16:36.083373070 CEST	53	64345	8.8.8.8	192.168.2.5
May 4, 2021 07:16:41.927670002 CEST	57128	53	192.168.2.5	8.8.8.8
May 4, 2021 07:16:41.984246016 CEST	53	57128	8.8.8.8	192.168.2.5
May 4, 2021 07:16:44.636957884 CEST	54791	53	192.168.2.5	8.8.8.8
May 4, 2021 07:16:44.687063932 CEST	53	54791	8.8.8.8	192.168.2.5
May 4, 2021 07:16:48.006705999 CEST	50463	53	192.168.2.5	8.8.8.8
May 4, 2021 07:16:48.068186045 CEST	53	50463	8.8.8.8	192.168.2.5
May 4, 2021 07:17:09.017355919 CEST	50394	53	192.168.2.5	8.8.8.8
May 4, 2021 07:17:09.074579000 CEST	53	50394	8.8.8.8	192.168.2.5
May 4, 2021 07:17:09.249906063 CEST	58530	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 07:17:09.306946993 CEST	53	58530	8.8.8.8	192.168.2.5
May 4, 2021 07:17:14.907283068 CEST	53813	53	192.168.2.5	8.8.8.8
May 4, 2021 07:17:14.964596987 CEST	53	53813	8.8.8.8	192.168.2.5
May 4, 2021 07:17:20.775229931 CEST	63732	53	192.168.2.5	8.8.8.8
May 4, 2021 07:17:20.834326982 CEST	53	63732	8.8.8.8	192.168.2.5
May 4, 2021 07:17:26.053299904 CEST	57344	53	192.168.2.5	8.8.8.8
May 4, 2021 07:17:26.105016947 CEST	53	57344	8.8.8.8	192.168.2.5
May 4, 2021 07:17:26.803852081 CEST	54450	53	192.168.2.5	8.8.8.8
May 4, 2021 07:17:26.878624916 CEST	53	54450	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 07:15:26.659554005 CEST	192.168.2.5	8.8.8.8	0xfde7	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
May 4, 2021 07:15:45.498770952 CEST	192.168.2.5	8.8.8.8	0x6c1b	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
May 4, 2021 07:16:03.390650034 CEST	192.168.2.5	8.8.8.8	0xac31	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
May 4, 2021 07:16:27.824098110 CEST	192.168.2.5	8.8.8.8	0x33b1	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
May 4, 2021 07:16:36.024789095 CEST	192.168.2.5	8.8.8.8	0xf2	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
May 4, 2021 07:16:41.927670002 CEST	192.168.2.5	8.8.8.8	0x94d8	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
May 4, 2021 07:17:09.017355919 CEST	192.168.2.5	8.8.8.8	0x1373	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
May 4, 2021 07:17:14.907283068 CEST	192.168.2.5	8.8.8.8	0xc554	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
May 4, 2021 07:17:20.775229931 CEST	192.168.2.5	8.8.8.8	0x4571	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)

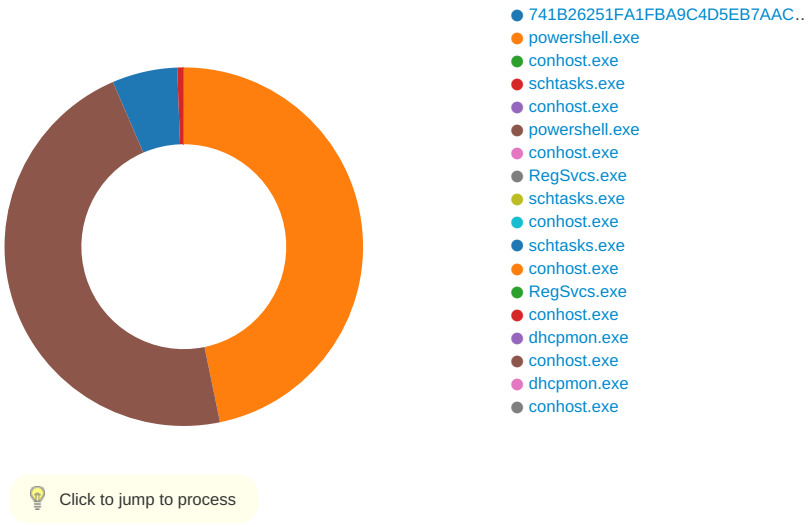
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 07:15:26.716960907 CEST	8.8.8.8	192.168.2.5	0xfde7	No error (0)	strongodss .ddns.net		79.134.225.82	A (IP address)	IN (0x0001)
May 4, 2021 07:15:45.557560921 CEST	8.8.8.8	192.168.2.5	0x6c1b	No error (0)	strongodss .ddns.net		79.134.225.82	A (IP address)	IN (0x0001)
May 4, 2021 07:16:03.449012995 CEST	8.8.8.8	192.168.2.5	0xac31	No error (0)	strongodss .ddns.net		79.134.225.82	A (IP address)	IN (0x0001)
May 4, 2021 07:16:27.882668018 CEST	8.8.8.8	192.168.2.5	0x33b1	No error (0)	strongodss .ddns.net		79.134.225.82	A (IP address)	IN (0x0001)
May 4, 2021 07:16:36.083373070 CEST	8.8.8.8	192.168.2.5	0xf2	No error (0)	strongodss .ddns.net		79.134.225.82	A (IP address)	IN (0x0001)
May 4, 2021 07:16:41.984246016 CEST	8.8.8.8	192.168.2.5	0x94d8	No error (0)	strongodss .ddns.net		79.134.225.82	A (IP address)	IN (0x0001)
May 4, 2021 07:17:09.074579000 CEST	8.8.8.8	192.168.2.5	0x1373	No error (0)	strongodss .ddns.net		79.134.225.82	A (IP address)	IN (0x0001)
May 4, 2021 07:17:14.964596987 CEST	8.8.8.8	192.168.2.5	0xc554	No error (0)	strongodss .ddns.net		79.134.225.82	A (IP address)	IN (0x0001)
May 4, 2021 07:17:20.834326982 CEST	8.8.8.8	192.168.2.5	0x4571	No error (0)	strongodss .ddns.net		79.134.225.82	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: 741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe PID: 6180 Parent PID: 5616

General

Start time:	07:15:30
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe'
Imagebase:	0xc20000
File size:	786944 bytes
MD5 hash:	CDDA16BD52C7C602B534593BE9149A42
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.244648700.000000000336A000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.248045352.00000000044C7000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.248045352.00000000044C7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.248045352.00000000044C7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\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	72B860AC	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	72B860AC	unknown
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	72B860AC	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	72B860AC	unknown
C:\Users\user\AppData\Roaming\gKpxRZsP.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	16C2E64	CopyFileW
C:\Users\user\AppData\Roaming\gKpxRZsP.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	16C2E64	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp30C2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	16C3050	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B734A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp30C2.tmp	success or wait	1	16C320A	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\gKpxRZsP.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 4e 3a 5f 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 f8 0b 00 00 08 00 00 00 00 00 00 52 16 0c 00 00 20 00 00 00 20 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...N:_`.......... ..................R.... ... ....@.. .......................` ....@................	success or wait	4	16C2E64	CopyFileW
C:\Users\user\AppData\Roaming\gKpxRZsP.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	16C2E64	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp30C2.tmp	unknown	1645	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationI	success or wait	1	16C0093	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe.log	unknown	1046	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	72E5A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	16C0093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	16C0093	ReadFile

Analysis Process: powershell.exe PID: 6356 Parent PID: 6180

General

Start time:	07:15:32
Start date:	04/05/2021
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\741B26251FA1FBA9C4D5EB7AACA544F07859F82C296B8.exe'
Imagebase:	0x9e0000
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	6D1DCF06	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	6D1DCF06	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	6BF85B28	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	6BF85B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y5ptkebd.tnb.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C021E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_eywfmlgy.1th.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C021E60	CreateFileW
C:\Users\user\Documents\20210504	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C02BEFF	CreateDirectoryW
C:\Users\user\Documents\20210504\PowerShell_transcript.813435.WJkwONF7.20210504071534.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C021E60	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	6C021E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y5ptkebd.tnb.ps1	success or wait	1	6C026A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_eywfmlgy.1th.psm1	success or wait	1	6C026A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y5ptkebd.tnb.ps1	unknown	1	31	1	success or wait	1	6C021B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_eywfmlgy.1th.psm1	unknown	1	31	1	success or wait	1	6C021B4F	WriteFile
C:\Users\user\Documents\20210504\PowerShell_transcript.813435.WJkwONF7.20210504071534.txt	unknown	3	ef bb bf	...	success or wait	1	6C021B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210504\PowerShell_transcript.813435.WJkwONF7.20210504071534.txt	unknown	707	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 35 30 34 30 37 31 35 35 34 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 38 31 33 34 33 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********..Windows PowerShell transcript start..Start time: 20210504071554..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 813435 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	44	6C021B4F	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\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6C021B4F	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-Runspac	success or wait	1	6C021B4F	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	6C021B4F	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-BitLockerRequiredActionsInternal........Unlock-PasswordInternal........Unlock-BitLocker........Add-TpmProtectorInternal....%...Add-RecoveryPasswordProtectorInternal.....Unlock-Recover	success or wait	1	6C021B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 6b 14 00 00 19 00 00 00 e9 0d f9 05 f0 07 e4 07 c4 07 00 00 00 00 52 02 36 00 c7 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....k.....R.6.....@.....	success or wait	1	6D4A76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 3a 00 00 00 0e 00 20 00	H.....<@.^...L."My....:..... .	success or wait	17	6D4A76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6D4A76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6D4A76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6D4A76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 54 01 40 00 f9 3e 40 01 cb 00 40 00 09 06 80 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 09 0c 80 00 58 64 40 01 56 64 40 01 fb 2a 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 16 3b 40 01 1b 3b 40 01 7a 54 40 01 95 54 40 01 19 3b 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 bc 3c 40 01 bd 3c 40 01 be 3c 40 01 57 03 40 01 4d 03 40 01 21 4d 40 01 b3 29 40 01 df 3f 40 01 a0 6f 40 01 a1 6f 40 01 a2 6f 40 01 f3 3f 40 01 f0 45 40 01 3b 4d 40	....T.@..>@...@.....V.@.H .@.X.@. [.@.NT@.HT@..S@..S@. hT@..S @..S@..S@.\.@..T@..T@. @X@.?X@. ....Xd@.Vd@..*@..T@..S @..S@..T @..T@.xT@..;@..;@.zT@. .T@..;@. =M@.DM@.:M@."M@. M@..<@..<@..< @.W.@.M.@.!M@..)@..? @..o@..o@..o@..? @..E@.;M@	success or wait	11	6D4A76FC	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	6D1B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D1B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D1BCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D1BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D1B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D1B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D1B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D1B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D1103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1B5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D1C1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21316	success or wait	1	6D1C203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1103DE	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	6C021B4F	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	6C021B4F	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	6C021B4F	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	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	136	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D1103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D1B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D1B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C021B4F	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	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D1B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D1B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C021B4F	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	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C021B4F	ReadFile

Analysis Process: conhost.exe PID: 6372 Parent PID: 6356

General

Start time:	07:15:33
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6412 Parent PID: 6180

General

Start time:	07:15:33
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\gKpxRZsP' /XML 'C:\Users\user\AppData\Local\Temp\tmp30C2.tmp'
Imagebase:	0x950000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp30C2.tmp	unknown	2	success or wait	1	95AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp30C2.tmp	unknown	1646	success or wait	1	95ABD9	ReadFile

Analysis Process: conhost.exe PID: 6472 Parent PID: 6412

General

Start time:	07:15:33
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 6528 Parent PID: 6180

General

Start time:	07:15:34
Start date:	04/05/2021
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\AppData\Roaming\gKpxRZsP.exe'
Imagebase:	0x9e0000
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	6D1DCF06	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	6D1DCF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y2xejyx0.1ov.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C021E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gof3hya4.2ip.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C021E60	CreateFileW
C:\Users\user\Documents\20210504\PowerShell_transcript.813435.K7iDO9IF.20210504071538.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C021E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y2xejyx0.1ov.ps1	success or wait	1	6C026A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gof3hya4.2ip.psm1	success or wait	1	6C026A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_y2xejyx0.1ov.ps1	unknown	1	31	1	success or wait	1	6C021B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gof3hya4.2ip.psm1	unknown	1	31	1	success or wait	1	6C021B4F	WriteFile
C:\Users\user\Documents\20210504\PowerShell_transcript.813435.K7iDO9IF.20210504071538.txt	unknown	3	ef bb bf	...	success or wait	1	6C021B4F	WriteFile
C:\Users\user\Documents\20210504\PowerShell_transcript.813435.K7iDO9IF.20210504071538.txt	unknown	678	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 35 30 34 30 37 31 35 35 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 38 31 33 34 33 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********..Windows PowerShell transcript start..Start time: 20210504071558..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 813435 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	44	6C021B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....<.e....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6C021B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.....Remove-Variable.....Convert-String.....Trace-Command.....Sort-Object.....Register-ObjectEvent.....Get-Runspace.....Format-Table.....Wait-Debugger.....Get-Runspac	success or wait	1	6C021B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 ce 12 09 ca 9f d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e........Install-PackageProvider........Import-PackageProvider........Get-PackageProvider.........Register-PackageSource.........Uninstall-Package.....Find-PackageProvider.....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	6C021B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2446	10 00 00 00 52 65 73 75 6d 65 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 1c 00 00 00 42 61 63 6b 75 70 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 25 00 00 00 53 68 6f 77 2d 42 69 74 4c 6f 63 6b 65 72 52 65 71 75 69 72 65 64 41 63 74 69 6f 6e 73 49 6e 74 65 72 6e 61 6c 02 00 00 00 17 00 00 00 55 6e 6c 6f 63 6b 2d 50 61 73 73 77 6f 72 64 49 6e 74 65 72 6e 61 6c 02 00 00 00 10 00 00 00 55 6e 6c 6f 63 6b 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 18 00 00 00 41 64 64 2d 54 70 6d 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 25 00 00 00 41 64 64 2d 52 65 63 6f 76 65 72 79 50 61 73 73 77 6f 72 64 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 55 6e 6c 6f 63 6b 2d 52 65 63 6f 76 65 72	....Resume-BitLocker........Backup-BitLockerKeyProtector....%...Show-BitLockerRequiredActionsInternal........Unlock-PasswordInternal........Unlock-BitLocker........Add-TpmProtectorInternal....%...Add-RecoveryPasswordProtectorInternal.....Unlock-Recover	success or wait	1	6C021B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 86 14 00 00 19 00 00 00 e9 0d 75 05 74 08 64 08 44 08 00 00 00 00 34 01 1c 00 c7 0d 00 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....u.t.d.D.....4.....@.....	success or wait	1	6D4A76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 52 00 00 00 0e 00 20 00	H.....<@.^...L."My.. .:R..... .	success or wait	17	6D4A76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6D4A76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6D4A76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6D4A76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 54 01 40 00 f9 3e 40 01 ce 67 40 01 99 01 40 00 fb 00 40 00 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 16 3b 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 1b 3b 40 01 19 3b 40 01 bc 3c 40 01 bd 3c 40 01 be 3c 40 01 57 03 40 01 4d 03 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 f0 45 40 01 40 4d 00 01 3c 4d 00 01 24 4d 00 01 38 4d 00 01 3f 4d 00	....T.@..>@..g@...@... @...@.V.@.H.@.X.@. [.@.NT@.HT@..S @..;@..S@.hT@..S@..S@ ..S@.\.@. .T@..T@.@X@.? X@..T@..S@..S@..T @..T@.xT@.zT@..T@.=M @.DM@.:M@."M@. M@..;@..;@..<@..<@.. <@.W. @.M.@.!M@.;M@..D@..D @..E@.@M.. <M..$M..8M..?M.	success or wait	11	6D4A76FC	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	6D1B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D1B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D1BCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D1BCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1103DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D1B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D1B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D1B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D1B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D1103DE	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	6D1B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6D1B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1B5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D1C1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21316	success or wait	1	6D1C203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1103DE	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	6C021B4F	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	6C021B4F	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	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	121	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C021B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D1103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1103DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D1B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D1B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	7	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D1B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D1B5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C021B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C021B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	2	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	15	6C021B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C021B4F	ReadFile

Analysis Process: conhost.exe PID: 6548 Parent PID: 6528

General

Start time:	07:15:34
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 6556 Parent PID: 6180

General

Start time:	07:15:34
Start date:	04/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0x7ff797770000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.511998017.000000000434C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.511998017.000000000434C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.513739140.0000000006030000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.513739140.0000000006030000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.513768537.0000000006040000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.513768537.0000000006040000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.513768537.0000000006040000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.501231522.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.501231522.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.501231522.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

Analysis Process: schtasks.exe PID: 6696 Parent PID: 6556

General

Start time:	07:15:37
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpB146.tmp'
Imagebase:	0x950000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6704 Parent PID: 6696

General

Start time:	07:15:37
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6756 Parent PID: 6556

General

Start time:	07:15:38
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpB52F.tmp'
Imagebase:	0x950000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6764 Parent PID: 6756

General

Start time:	07:15:38
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 6856 Parent PID: 904

General

Start time:	07:15:40
Start date:	04/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0
Imagebase:	0x7c0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6864 Parent PID: 6856

General

Start time:	07:15:40
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 6872 Parent PID: 904

General

Start time:	07:15:40
Start date:	04/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x440000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: conhost.exe PID: 6884 Parent PID: 6872

General

Start time:	07:15:40
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 5732 Parent PID: 3472

General

Start time:	07:15:48
Start date:	04/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x180000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 5928 Parent PID: 5732

General

Start time:	07:15:48
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis