ID: 411771
Sample Name: Devizni izvod za partiju 0050100073053.exe
Cookbook: default.jbs
Time: 06:29:53
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

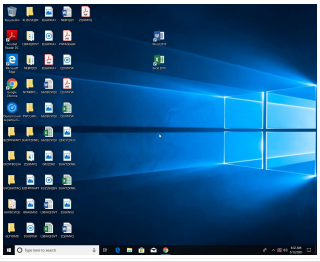
Analysis Report Devizni izvod za partiju 0050100073053…

Overview

General Information

Sample Name:	Devizni izvod za partiju 0050100073053.exe
Analysis ID:	411771
MD5:	50ab414be17f4e0.
SHA1:	d0def6e40e7858a.
SHA256:	333b1ae9552e6a..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

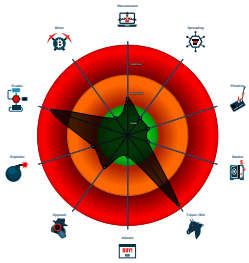
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- Adds a directory exclusion to Windo…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…

Classification



Startup

- **System is w10x64**
- Devizni izvod za partiju 0050100073053.exe (PID: 4504 cmdline: 'C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe' MD5: 50AB414BE17F4E03BEE8F9C5CEE06335)
  - powershell.exe (PID: 5488 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5304 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5876 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\AGYVBigGPY.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 1744 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\AGYVBigGPY' /XML 'C:\Users\user\AppData\Local\Temp\tmp2011.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5852 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 2104 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\AGYVBigGPY.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5340 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Devizni izvod za partiju 0050100073053.exe (PID: 5932 cmdline: C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe MD5: 50AB414BE17F4E03BEE8F9C5CEE06335)
  - Devizni izvod za partiju 0050100073053.exe (PID: 6164 cmdline: C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe MD5: 50AB414BE17F4E03BEE8F9C5CEE06335)
  - Devizni izvod za partiju 0050100073053.exe (PID: 6196 cmdline: C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe MD5: 50AB414BE17F4E03BEE8F9C5CEE06335)
- dhcpmon.exe (PID: 6792 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 50AB414BE17F4E03BEE8F9C5CEE06335)
  - powershell.exe (PID: 4708 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6076 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6092 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\AGYVBigGPY' /XML 'C:\Users\user\AppData\Local\Temp\tmp864D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6644 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\AGYVBigGPY.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1880 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 4608 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 50AB414BE17F4E03BEE8F9C5CEE06335)
  - dhcpmon.exe (PID: 5356 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 50AB414BE17F4E03BEE8F9C5CEE06335)
  - dhcpmon.exe (PID: 900 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 50AB414BE17F4E03BEE8F9C5CEE06335)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "b90524a1-4a4b-41de-ac06-59066a86",
  "Group": "Panda",
  "Domain1": "emedoo.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 5230,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 50,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "emedoo.ddns.net",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000003.296886935.000000000404 0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000D.00000003.296886935.000000000404 0000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1151:$a: NanoCore • 0x11aa:$a: NanoCore • 0x11e7:$a: NanoCore • 0x1260:$a: NanoCore • 0x1490b:$a: NanoCore • 0x14920:$a: NanoCore • 0x14955:$a: NanoCore • 0x1e7b9:$a: NanoCore • 0x1e812:$a: NanoCore • 0x1e84f:$a: NanoCore • 0x1e8c8:$a: NanoCore • 0x31f73:$a: NanoCore • 0x31f88:$a: NanoCore • 0x31fbd:$a: NanoCore • 0x3fbd2:$a: NanoCore • 0x3fbf7:$a: NanoCore • 0x3fc50:$a: NanoCore • 0x11b3:$b: ClientPlugin • 0x11f0:$b: ClientPlugin • 0x1aee:$b: ClientPlugin • 0x1afb:$b: ClientPlugin
0000000D.00000002.541194418.0000000003D8 D000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000013.00000002.373412048.000000000476 1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x891dd:$x1: NanoCore.ClientPluginHost • 0x8921a:$x2: IClientNetworkHost • 0x8cd4d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000013.00000002.373412048.000000000476 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 51 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.Devizni izvod za partiju 0050100073053.exe.2dc23b0.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x8ba5:$x1: NanoCore.ClientPluginHost • 0x15d17:$x1: NanoCore.ClientPluginHost • 0x1fb6f:$x1: NanoCore.ClientPluginHost • 0x27a9d:$x1: NanoCore.ClientPluginHost • 0x2da78:$x1: NanoCore.ClientPluginHost • 0x374eb:$x1: NanoCore.ClientPluginHost • 0x4191f:$x1: NanoCore.ClientPluginHost • 0x4c909:$x1: NanoCore.ClientPluginHost • 0x586b7:$x1: NanoCore.ClientPluginHost • 0x6440a:$x1: NanoCore.ClientPluginHost • 0x8bd2:$x2: IClientNetworkHost • 0x15d50:$x2: IClientNetworkHost • 0x1fba8:$x2: IClientNetworkHost • 0x27ad6:$x2: IClientNetworkHost • 0x37648:$x2: IClientNetworkHost • 0x41958:$x2: IClientNetworkHost • 0x4c923:$x2: IClientNetworkHost • 0x586d1:$x2: IClientNetworkHost • 0x64447:$x2: IClientNetworkHost
13.2.Devizni izvod za partiju 0050100073053.exe.2dc23b0.4.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x8b7f:$a: NanoCore • 0x8ba5:$a: NanoCore • 0x8c01:$a: NanoCore • 0x15a5f:$a: NanoCore • 0x15ab8:$a: NanoCore • 0x15aeb:$a: NanoCore • 0x15d17:$a: NanoCore • 0x15d93:$a: NanoCore • 0x163ac:$a: NanoCore • 0x164f5:$a: NanoCore • 0x169c9:$a: NanoCore • 0x16cb0:$a: NanoCore • 0x16cc7:$a: NanoCore • 0x1fb6f:$a: NanoCore • 0x1fbeb:$a: NanoCore • 0x224ce:$a: NanoCore • 0x27a9d:$a: NanoCore • 0x27b17:$a: NanoCore • 0x2da78:$a: NanoCore • 0x2dac2:$a: NanoCore • 0x2e71c:$a: NanoCore
34.2.dhcpmon.exe.3f0e434.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0x28271:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost • 0x2829e:$x2: IClientNetworkHost
34.2.dhcpmon.exe.3f0e434.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x28271:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0x2934c:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost • 0x2828b:$s5: IClientLoggingHost
34.2.dhcpmon.exe.3f0e434.6.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 168 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Non Interactive PowerShell

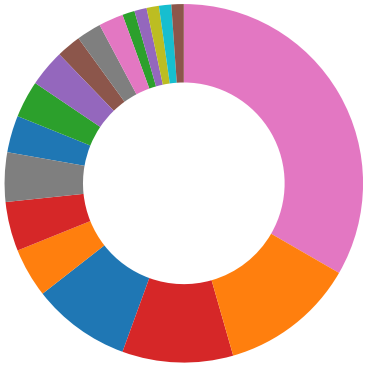
Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

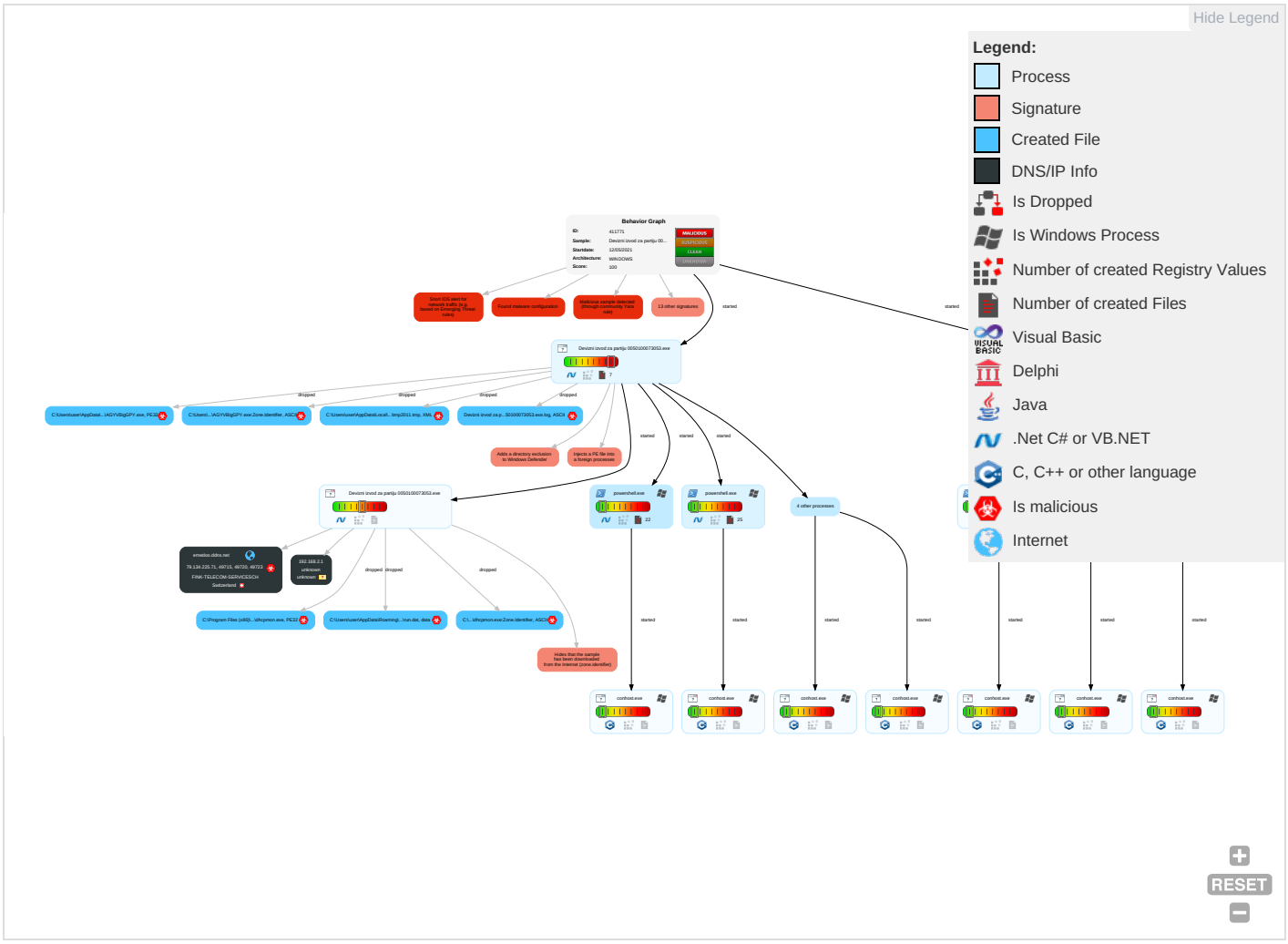
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	E I N C
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Obfuscated Files or Information 3	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1	E F C
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Software Packing 3	Security Account Manager	System Information Discovery 1 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 2	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 3 1	LSA Secrets	Security Software Discovery 2 2 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 1	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 2 1	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Virtualization/Sandbox Evasion 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	F A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D I F

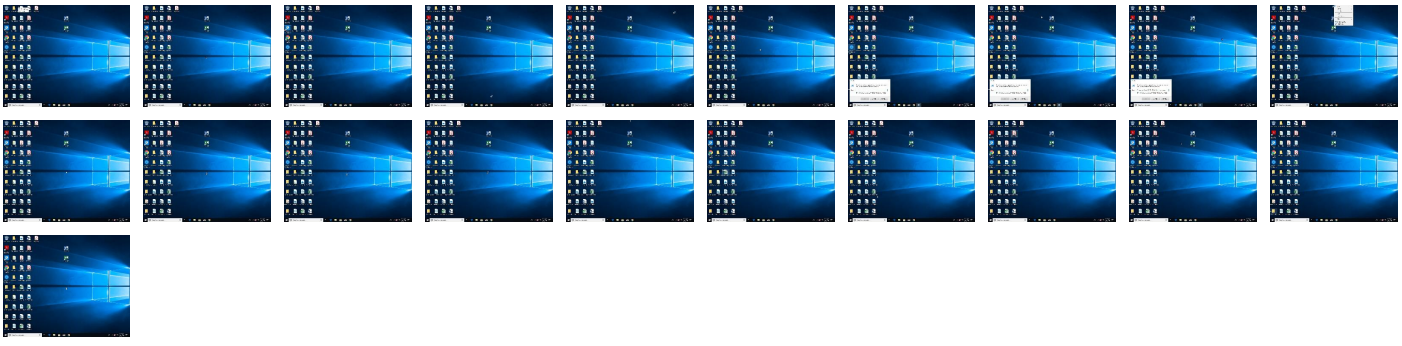
Behavior Graph



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
Devizni izvod za partiju 0050100073053.exe	66%	Virustotal		Browse
Devizni izvod za partiju 0050100073053.exe	24%	Metadefender		Browse
Devizni izvod za partiju 0050100073053.exe	48%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
Devizni izvod za partiju 0050100073053.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\AGYVBigGPY.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	24%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	48%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
C:\Users\user\AppData\Roaming\AGYVBigGPY.exe	24%	Metadefender		Browse
C:\Users\user\AppData\Roaming\AGYVBigGPY.exe	48%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.2.Devizni izvod za partiju 0050100073053.exe.56b0000.23.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Source	Detection	Scanner	Label	Link	Download
34.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.2.Devizni izvod za partiju 0050100073053.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://im.twitvid.com/api/upload	0%	Virustotal		Browse
http://im.twitvid.com/api/upload	0%	Avira URL Cloud	safe	
http://twic.li/api/uploadAudioAndTweet	0%	Avira URL Cloud	safe	
http://twic.li/api/video.flv?id=-No	0%	Avira URL Cloud	safe	
http://yfrog.com/api/uploadAndPostAmultipart/form-data	0%	Avira URL Cloud	safe	
http://https://im.twitvid.com/api/authenticate	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://twic.li/api/uploadVideoAndTweet	0%	Avira URL Cloud	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://twic.li/api/photo.jpg?id=	0%	Avira URL Cloud	safe	
http://twic.li/api/getUsersContent?userid=)&content_type=photos	0%	Avira URL Cloud	safe	
http://twic.li/api/getUsersContent?userid=	0%	Avira URL Cloud	safe	
http://twic.li/api/uploadPhotoAndTweet	0%	Avira URL Cloud	safe	
http://twic.li/api/getContent?id=	0%	Avira URL Cloud	safe	
emedoo.ddns.net	0%	Avira URL Cloud	safe	
http://twic.li/api/uploadAudio	0%	Avira URL Cloud	safe	
http://yfrog.com/api/uploadAndPost	0%	Avira URL Cloud	safe	
http://twic.li/api/uploadAudioiContent-disposition:	0%	Avira URL Cloud	safe	
http://twic.li/api/video.flv?id=	0%	Avira URL Cloud	safe	
http://twic.li/api/getUsersContent?username=	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://twic.li/api/uploadAudioAndTweetUContent-Disposition:	0%	Avira URL Cloud	safe	
http://https://im.twitvid.com/api/authenticateCapplication/x-www-form-urlencoded	0%	Avira URL Cloud	safe	
http://twic.li/api/uploadVideoLhttp://twic.li/api/uploadVideoAndTweet	0%	Avira URL Cloud	safe	
http://twic.li/api/uploadVideo	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://twic.li/api/uploadPhoto	0%	Avira URL Cloud	safe	
http://twic.li/api/uploadPhotokContent-Disposition:	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Avira URL Cloud	safe	
http://twic.li/api/uploadAudioLhttp://twic.li/api/uploadAudioAndTweet:http://twic.li/api/getContentD	0%	Avira URL Cloud	safe	
http://twic.li/api/uploadPhotoLhttp://twic.li/api/uploadPhotoAndTweet	0%	Avira URL Cloud	safe	
http://im.twitvid.com/api/uploadrhttp://api.twitter.com/1.1/account/verify_credentials.xmljhttp://ap	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
emedoo.ddns.net	79.134.225.71	true	true	• 5%, Virustotal, Browse	unknown

Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://im.twitvid.com/api/upload	Devizni izvod za partiju 00501 00073053.exe, Devizni izvod za partiju 0 050100073053.exe, 0000000D.000 00000.247851336.00000000005820 00.00000002.00020000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://api.twitter.com/1.1/statuses/mentions.xml	Devizni izvod za partiju 00501 00073053.exe	false		high
http:// api.twitter.com/1.1/blocks/blocking.xmldhttp://api.twitter.com/1. 1/blocks/blocking/ids.xml	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false		high
http://api.twitter.com/1.1/statuses/retweeted_by_me.xml	Devizni izvod za partiju 00501 00073053.exe, Devizni izvod za partiju 0 050100073053.exe, 0000000D.000 00000.247851336.00000000005820 00.00000002.00020000.sdmp	false		high
http://api.twitter.com/1.1/statuses/friends_timeline.xml	Devizni izvod za partiju 00501 00073053.exe	false		high
http://api.twitter.com/1.1/direct_messages.xml	Devizni izvod za partiju 00501 00073053.exe	false		high
http://twic.li/api/uploadAudioAndTweet	Devizni izvod za partiju 00501 00073053.exe	false	• Avira URL Cloud: safe	unknown
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstr ap.min.css	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 2.255288442.0000000002A3B000.0 0000004.00000001.sdmp	false		high
http://api.twitter.com/1.1/blocks/destroy/	Devizni izvod za partiju 00501 00073053.exe, 0000000D.0000000 0.247851336.0000000000582000.0 0000002.00020000.sdmp	false		high
http:// api.twitter.com/1.1/direct_messages/new.xmlfhttp://api.twitter.c om/1.1/direct_messages/sent.x	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false		high
http:// api.twitter.com/1.1/report_spam.xmlJhttp://search.twitter.com/s earch.atomfhttp://api.twitter.	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://twic.li/api/video.flv?id=-No	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false	• Avira URL Cloud: safe	unknown
http://api.twitter.com/1.1/account/update_profile.xml	Devizni izvod za partiju 00501 00073053.exe	false		high
http://yfrog.com/api/uploadAndPostAmultipart/form-data	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false	• Avira URL Cloud: safe	unknown
http://api.twitter.com/1.1/statuses/show/	Devizni izvod za partiju 00501 00073053.exe, Devizni izvod za partiju 0 050100073053.exe, 0000000D.000 00000.247851336.00000000005820 00.00000002.00020000.sdmp	false		high
http://api.twitter.com/1.1/friendships/show.xml?	Devizni izvod za partiju 00501 00073053.exe, 0000000D.0000000 0.247851336.0000000000582000.0 0000002.00020000.sdmp	false		high
http://https://nuget.org/nuget.exe	powershell.exe, 00000005.00000 002.543192744.0000000006172000 .00000004.00000001.sdmp, power shell.exe, 00000009.00000002.5 45169249.00000000055F3000.0000 0004.00000001.sdmp	false		high
http://search.twitter.com/trends/current.json	Devizni izvod za partiju 00501 00073053.exe	false		high
http://api.twitter.com/1.1/statuses/friends.xml	Devizni izvod za partiju 00501 00073053.exe	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000003.00000 002.532843494.0000000004F41000 .00000004.00000001.sdmp, power shell.exe, 00000005.00000002.5 32258311.0000000005111000.0000 0004.00000001.sdmp, powershell.exe, 00000009.00000002.534281663.000000 0004591000.00000004.00000001.sdmp	false		high
http://api.twitter.com/1.1/report_spam.xml	Devizni izvod za partiju 00501 00073053.exe	false		high
http://https://im.twitvid.com/api/authenticate	Devizni izvod za partiju 00501 00073053.exe, Devizni izvod za partiju 0 050100073053.exe, 0000000D.000 00000.247851336.00000000005820 00.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://twitter.com/oauth/request_token-	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://api.twitter.com/1.1/statuses/destroy/	Devizni izvod za partiju 00501 00073053.exe, Devizni izvod za partiju 0 050100073053.exe, 0000000D.000 00000.247851336.00000000005820 00.00000002.00020000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000005.00000 002.535788541.0000000005251000 .00000004.00000001.sdmp, power shell.exe, 00000009.00000003.4 30789624.0000000007721000.0000 0004.00000001.sdmp, powershell.exe, 00000009.00000002.538651440.000000 00046D7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000003.00000 002.537074533.0000000005083000 .00000004.00000001.sdmp, power shell.exe, 00000005.00000002.5 35788541.0000000005251000.0000 0004.00000001.sdmp, powershell.exe, 00000009.00000002.538651440.000000 00046D7000.00000004.00000001.sdmp	false		high
http://twitter.com/oauth/access_token#?x_auth_username=#&x_auth_password=1&x_auth_mode=client_authUh	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000005.00000 002.535788541.0000000005251000 .00000004.00000001.sdmp, power shell.exe, 00000009.00000003.4 30789624.0000000007721000.0000 0004.00000001.sdmp, powershell.exe, 00000009.00000002.538651440.000000 00046D7000.00000004.00000001.sdmp	false		high
http://api.twitter.com/1.1/statuses/public_timeline.xml	Devizni izvod za partiju 00501 00073053.exe	false		high
http://https://go.micro	powershell.exe, 00000003.00000 003.415909540.00000000058E5000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api.twitter.com/1.1/trends/available.xmlThttp://api.twitter.com/1.1/trends/	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false		high
http://api.twitter.com/1.1/account/update_profile.xmlQhttp://api.twitter.com/1.1/favorites.xmlghttp:	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false		high
http://twic.li/api/uploadVideoAndTweet	Devizni izvod za partiju 00501 00073053.exe, Devizni izvod za partiju 0 050100073053.exe, 0000000D.000 00000.247851336.00000000005820 00.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://contoso.com/Icon	powershell.exe, 00000009.00000002.545169249.00000000055F3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api.twitter.com/1.1/direct_messages/sent.xml	Devizni izvod za partiju 00501 00073053.exe	false		high
http://api.twitter.com/1.1/favorites/destroy/	Devizni izvod za partiju 00501 00073053.exe, 0000000D.00000000.247851336.0000000000582000.00000002.00020000.sdmp	false		high
http://api.twitter.com/1.1/trends/available.xml	Devizni izvod za partiju 00501 00073053.exe	false		high
http://twic.li/api/photo.jpg?id=	Devizni izvod za partiju 00501 00073053.exe, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336.0000000000582000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://twic.li/api/getUsersContent?userid=)&content_type=photos	Devizni izvod za partiju 00501 00073053.exe, 00000002.00000000.233483406.0000000000262000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 00000000A.00000002.245256892.00000000002A2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.00000000.246259331.0000000000432000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336.0000000000582000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://twic.li/api/getUsersContent?userid=	Devizni izvod za partiju 00501 00073053.exe	false	• Avira URL Cloud: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000005.00000002.535788541.0000000005251000.00000004.00000001.sdmp, powershell.exe, 00000009.00000003.430789624.0000000007721000.00000004.00000001.sdmp, powershell.exe, 00000009.00000002.538651440.00000000046D7000.00000004.00000001.sdmp	false		high
http://api.twitter.com/1.1/favorites/create/	Devizni izvod za partiju 00501 00073053.exe	false		high
http://twic.li/api/uploadPhotoAndTweet	Devizni izvod za partiju 00501 00073053.exe, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336.0000000000582000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://api.twitter.com/1.1/statuses/replies.xml	Devizni izvod za partiju 00501 00073053.exe	false		high
http://api.twitter.com/1.1/statuses/friends.xmlbhttp://api.twitter.com/1.1/statuses/followers.xmlpht	Devizni izvod za partiju 00501 00073053.exe, 00000002.00000000.233483406.0000000000262000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 00000000A.00000002.245256892.00000000002A2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.00000000.246259331.0000000000432000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336.0000000000582000.00000002.00020000.sdmp	false		high
http://twic.li/api/getContent?id=	Devizni izvod za partiju 00501 00073053.exe, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336.0000000000582000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://api.twitter.com/1.1/account/update_profile_image.xml	Devizni izvod za partiju 00501 00073053.exe, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336.0000000000582000.00000002.00020000.sdmp	false		high
http://api.twitter.com/1.1/users/show.xml	Devizni izvod za partiju 00501 00073053.exe	false		high
http://twitter.com/oauth/request_token	Devizni izvod za partiju 00501 00073053.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000003.00000002.537074533.0000000005083000.00000004.00000001.sdmp, powershell.exe, 00000005.00000002.535788541.0000000005251000.00000004.00000001.sdmp, powershell.exe, 00000009.00000002.538651440.000000000046D7000.00000004.00000001.sdmp	false		high
http://api.twitter.com/1.1/direct_messages/destroy/	Devizni izvod za partiju 0050100073053.exe, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336.0000000000582000.00000002.00020000.sdmp	false		high
http://twic.li/api/uploadAudio	Devizni izvod za partiju 0050100073053.exe	false	• Avira URL Cloud: safe	unknown
http://api.twitter.com/1.1/direct_messages/new.xml?user=	Devizni izvod za partiju 0050100073053.exe, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336.0000000000582000.00000002.00020000.sdmp	false		high
http://twitter.com/oauth/access_token	Devizni izvod za partiju 0050100073053.exe	false		high
http://yfrog.com/api/uploadAndPost	Devizni izvod za partiju 0050100073053.exe, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336.0000000000582000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://twic.li/api/uploadAudioiContent-disposition:	Devizni izvod za partiju 0050100073053.exe, 00000002.00000000.233483406.0000000000262000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000A.00000002.245256892.00000000002A2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.00000000.246259331.0000000000432000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336.0000000000582000.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://api.twitter.com/1.1/users/search.xmlRhttp://api.twitter.com/1.1/users/show.xmlvhttp://api.twi	Devizni izvod za partiju 0050100073053.exe, 00000002.00000000.233483406.0000000000262000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000A.00000002.245256892.00000000002A2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.00000000.246259331.0000000000432000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336.0000000000582000.00000002.00020000.sdmp	false		high
http://api.twitter.com/1.1/statuses/replies.xmlfhttp://api.twitter.com/1.1/statuses/retweet/	Devizni izvod za partiju 0050100073053.exe, 00000002.00000000.233483406.0000000000262000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000A.00000002.245256892.00000000002A2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.00000000.246259331.0000000000432000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336.0000000000582000.00000002.00020000.sdmp	false		high
http://api.twitter.com/1.1/blocks/blocking.xml	Devizni izvod za partiju 0050100073053.exe	false		high

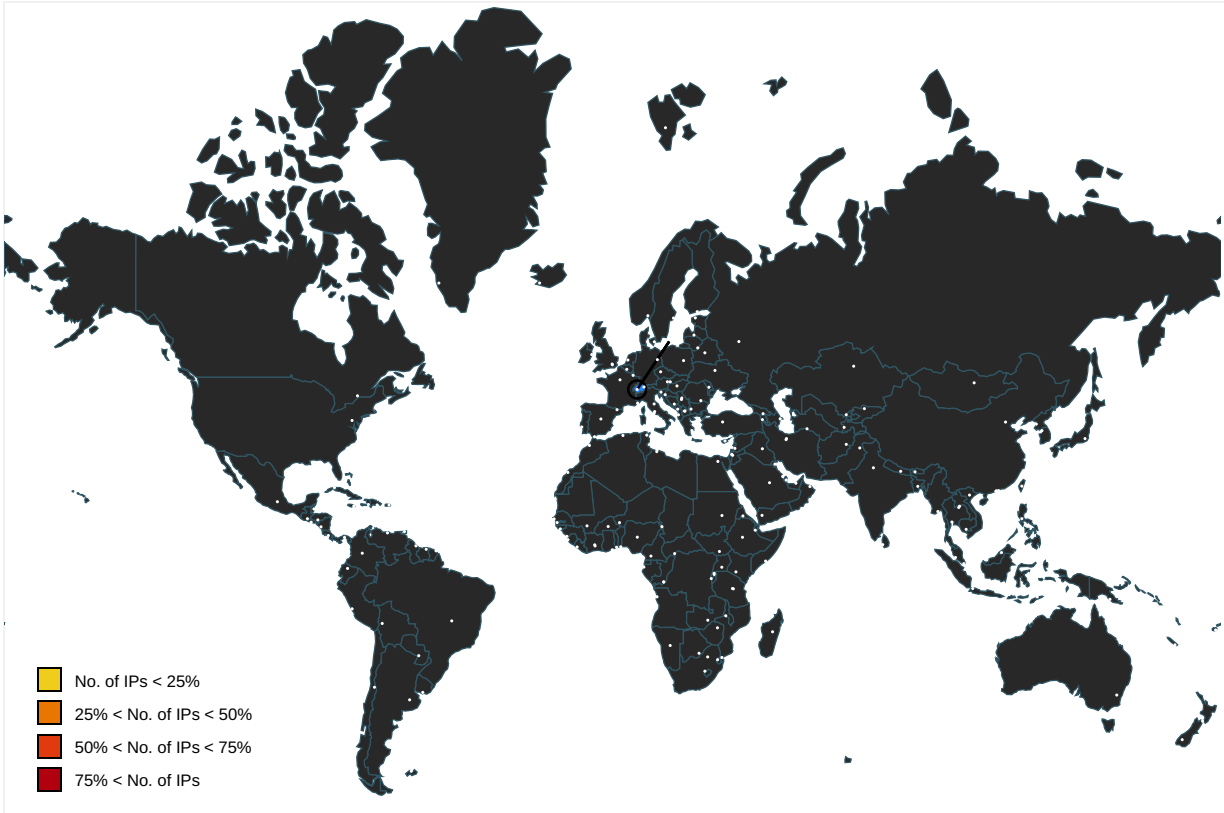
Name	Source	Malicious	Antivirus Detection	Reputation
http://twitter.com/statuses/retweeted_to_me.xmlfhttp://api.twitter.com/1.1/statuses/retweets/id.xmll	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false		high
http://api.twitter.com/1.1/	Devizni izvod za partiju 00501 00073053.exe, 0000000D.0000000 0.247851336.0000000000582000.0 0000002.00020000.sdmp	false		high
http://search.twitter.com/search.atom	Devizni izvod za partiju 00501 00073053.exe	false		high
http://twic.li/api/video.flv?id=	Devizni izvod za partiju 00501 00073053.exe	false	• Avira URL Cloud: safe	unknown
http://twic.li/api/getUsersContent?username=	Devizni izvod za partiju 00501 00073053.exe, Devizni izvod za partiju 0 050100073053.exe, 0000000D.000 00000.247851336.00000000005820 00.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/Pester/PesterH	powershell.exe, 00000003.00000 002.537074533.0000000005083000 .00000004.00000001.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000009.00000 002.545169249.00000000055F3000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api.twitter.com/1.1/statuses/mentions.xmlnhttp://api.twitter.com/1.1/statuses/public_timeline	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false		high
http://api.twitter.com/1.1/friendships/destroy/	Devizni izvod za partiju 00501 00073053.exe, 0000000D.0000000 0.247851336.0000000000582000.0 0000002.00020000.sdmp	false		high
http://api.twitter.com/1.1/statuses/update.xml?status=	Devizni izvod za partiju 00501 00073053.exe, Devizni izvod za partiju 0 050100073053.exe, 0000000D.000 00000.247851336.00000000005820 00.00000002.00020000.sdmp	false		high
http://twic.li/api/uploadAudioAndTweetUContent-Disposition:	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://im.twitvid.com/api/authenticateCapplication/x-www-form-urlencoded	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// twic.li/api/uploadVideoLhttp://twic.li/api/uploadVideoAndTweet	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.twitter.com/trends/weekly.json	Devizni izvod za partiju 00501 00073053.exe	false		high
http://https://api.twitter.com/oauth/access_token	Devizni izvod za partiju 00501 00073053.exe, Devizni izvod za partiju 0 050100073053.exe, 0000000D.000 00000.247851336.00000000005820 00.00000002.00020000.sdmp	false		high
http:// search.twitter.com/search.atomKhttp://search.twitter.com/trends.json	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false		high
http://twic.li/api/uploadVideo	Devizni izvod za partiju 00501 00073053.exe, Devizni izvod za partiju 0 050100073053.exe, 0000000D.000 00000.247851336.00000000005820 00.00000002.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/	powershell.exe, 00000009.00000 002.545169249.00000000055F3000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://twic.li/api/uploadPhoto	Devizni izvod za partiju 00501 00073053.exe	false	• Avira URL Cloud: safe	unknown
http://api.twitter.com/1.1/blocks/create/	Devizni izvod za partiju 00501 00073053.exe, 0000000D.0000000 0.247851336.0000000000582000.0 0000002.00020000.sdmp	false		high
http://api.twitter.com/1.1/statuses/retweet/	Devizni izvod za partiju 00501 00073053.exe, Devizni izvod za partiju 0 050100073053.exe, 0000000D.000 00000.247851336.00000000005820 00.00000002.00020000.sdmp	false		high
http://api.twitter.com/1.1/blocks/blocking/ids.xml	Devizni izvod za partiju 00501 00073053.exe, Devizni izvod za partiju 0 050100073053.exe, 0000000D.000 00000.247851336.00000000005820 00.00000002.00020000.sdmp	false		high
http://api.twitter.com/1.1/favorites.xml	Devizni izvod za partiju 00501 00073053.exe	false		high
http://api.twitter.com/1.1/statuses/home_timeline.xml	Devizni izvod za partiju 00501 00073053.exe	false		high
http://api.twitter.com/1.1/account/verify_credentials.xml	Devizni izvod za partiju 00501 00073053.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://twic.li/api/uploadPhotokContent-Disposition:	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false	• Avira URL Cloud: safe	unknown
http://api.twitter.com/1.1/trends/	Devizni izvod za partiju 00501 00073053.exe	false		high
http://api.twitter.com/1.1/statuses/retweets_of_me.xml	Devizni izvod za partiju 00501 00073053.exe	false		high
http://nuget.org/NuGet.exe	powershell.exe, 00000005.00000 002.543192744.0000000006172000 .00000004.00000001.sdmp, power shell.exe, 00000009.00000002.5 45169249.00000000055F3000.0000 0004.00000001.sdmp	false		high
http:// twic.li/api/uploadAudioLhttp://twic.li/api/uploadAudioAndTweet: http://twic.li/api/getContentD	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false	• Avira URL Cloud: safe	unknown
http://twitter.com/statuses/retweeted_to_me.xml	Devizni izvod za partiju 00501 00073053.exe	false		high
http://api.twitter.com/1.1/followers/ids.xml	Devizni izvod za partiju 00501 00073053.exe	false		high
http://www.apache.org/licenses/LICENSE-2.0.htmlH	powershell.exe, 00000003.00000 002.537074533.0000000005083000 .00000004.00000001.sdmp	false		high
http:// api.twitter.com/1.1/statuses/update.xmljhttp://api.twitter.com/1. 1/statuses/user_timeline.xml	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false		high
http:// twic.li/api/uploadPhotoLhttp://twic.li/api/uploadPhotoAndTweet	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://api.twitter.com/1.1/statuses/retweets/id.xml_http://api.twitter.com/1.1/statuses/replies.xmlS	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false		high
http://api.twitter.com/1.1/favorites.xmlXhttp://api.twitter.com/1.1/followers/ids.xmlThttp://api.twi	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false		high
http://im.twitvid.com/api/uploadrhttp://api.twitter.com/1.1/account/verify_credentials.xmljhttp://ap	Devizni izvod za partiju 00501 00073053.exe, 00000002.0000000 0.233483406.0000000000262000.0 0000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 000 0000A.00000002.245256892.00000 000002A2000.00000002.00020000. sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000C.0 0000000.246259331.000000000043 2000.00000002.00020000.sdmp, Devizni izvod za partiju 0050100073053.exe, 0000000D.00000000.247851336 .0000000000582000.00000002.000 20000.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.twitter.com/trends.json	Devizni izvod za partiju 00501 00073053.exe	false		high

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	411771
Start date:	12.05.2021
Start time:	06:29:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Devizni izvod za partiju 0050100073053.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:	39
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@35/31@9/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.2%) • Quality average: 64.8% • Quality standard deviation: 32.4%
HCA Information:	• Successful, ratio: 97% • 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 • Report creation exceeded maximum time and may have missing disassembly code information. • TCP Packets have been reduced to 100 • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
06:30:44	API Interceptor	355x Sleep call for process: Devizni izvod za partiju 0050100073053.exe modified
06:30:58	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
06:31:09	API Interceptor	1x Sleep call for process: dhcpmon.exe modified
06:31:44	API Interceptor	185x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.71	QwUl4FaToe.exe	Get hash	malicious	Browse	
	SCAN ORDER DOC 040202021.exe	Get hash	malicious	Browse	
	gfcYixSdyD.exe	Get hash	malicious	Browse	
	WxTm2cWLHF.exe	Get hash	malicious	Browse	
	uHAHxir7cFIdUqL.exe	Get hash	malicious	Browse	
	Wrcpl1dkib.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	Swift-EUR 28700.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	PAYMENT NOTIFICATION.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	fakture.exe	Get hash	malicious	Browse	
	BACK ORDER EXPORT0026254E_DOC_PDF.exe	Get hash	malicious	Browse	
	img_Payment Advice_822020_jpg.exe	Get hash	malicious	Browse	
	Bank Swift_7312020_PDF.exe	Get hash	malicious	Browse	
	LKVQYCZZkBgadMX.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	QwUl4FaToe.exe	Get hash	malicious	Browse	• 79.134.225.71
	IMG_1035852_607.exe	Get hash	malicious	Browse	• 79.134.225.10
	RFQEMFA.Elektrik.exe	Get hash	malicious	Browse	• 79.134.225.17
	Waybill Document 22700456.exe	Get hash	malicious	Browse	• 79.134.225.7
	Give Offer CVE6535 _TVOP-MIO, pdf.exe	Get hash	malicious	Browse	• 79.134.225.8
	Waybill Document 22700456.exe	Get hash	malicious	Browse	• 79.134.225.7
	RFQEMFA.Elektrik.pdf.exe	Get hash	malicious	Browse	• 79.134.225.17
	w85rzxid7y.exe	Get hash	malicious	Browse	• 79.134.225.81
	Remittance E-MAIL Layout - 10_.jar	Get hash	malicious	Browse	• 79.134.225.106
	s65eJyjKga.exe	Get hash	malicious	Browse	• 79.134.225.47
	new order.xlsx	Get hash	malicious	Browse	• 79.134.225.47
	Ot3srIM10B.exe	Get hash	malicious	Browse	• 79.134.225.47
	Remittance E-MAIL Layout - 10_.jar	Get hash	malicious	Browse	• 79.134.225.106
	wnQXyfONbS.exe	Get hash	malicious	Browse	• 79.134.225.82
	kwK4iGa9DL.exe	Get hash	malicious	Browse	• 79.134.225.47
	Remittance E-MAIL Layout - 10_.jar	Get hash	malicious	Browse	• 79.134.225.106

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	4z9Saf2vu3.exe	Get hash	malicious	Browse	• 79.134.225.47
	NewOrderSupplypdf.exe	Get hash	malicious	Browse	• 79.134.225.52
	Pu5UMH4fWK.exe	Get hash	malicious	Browse	• 79.134.225.14
	Swift-Correction.exe	Get hash	malicious	Browse	• 79.134.225.19

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	877568
Entropy (8bit):	7.25401903162754
Encrypted:	false
SSDEEP:	24576:0lO/1fBDLs8i4Y77/21nEgEcJCHwpKCfLc:0s/1pRY77/Lnc8HwlLc
MD5:	50AB414BE17F4E03BEE8F9C5CEE06335
SHA1:	D0DEF6E40E7858A1B8C46D46F24A6B29499C7C37
SHA-256:	333B1AE9552E6A65AB7C4EDEE6677746E801EBED73294795B9057E17A0E284E6
SHA-512:	A397E7DCEF69FBD15A51080CA4F6AC2A698C9B880D0773950BD7C7777DFC2C5436A084694A825A60CD638E0B637599EE2C9A08119709FF62BBB89374A92361D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 24%, Browse • Antivirus: ReversingLabs, Detection: 48%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....`..... ... ...@....@.. ....@.....0 ..O....@..`]..... ..... ..H.....text..... ..... ..`.rsrc...`]...@...^.....@..@.rel oc.....b.....@..B.....d .....H.....T}..TI.....e.....Y.....(...*&..(!....*.s".....s#.....s$.....s%.....s&.....*...0.....~....o'....+..*.0..... .....~....o(....+..*.0.....~....o)....+..*.0.....~....o*....+..*.0..<.....~.....(,.....,!r...p.....(-...o....s/.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r'.. p~....o0...(1.....t#....+..*...0..&.....(....r_..p~....o0...(1.....

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

Process:	C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Devizni izvod za partiju 0050100073053.exe.log

Process:	C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Devizni izvod za partiju 0050100073053.exe.log	
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
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\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",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:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
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\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	25168
Entropy (8bit):	4.975582086060887
Encrypted:	false
SSDEEP:	768:6BV3IpNBQkj2Lh4iUxQedNYotBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYoI:6BV3CNBQkj2Lh4iUxvdNYotBV3CNBQkx
MD5:	62E1AE94DE84ED9286704EBD6856A263
SHA1:	4888C4CFAA74FA9BCD7339CBF760B1060314246B
SHA-256:	9AC3E181F8EB940093EF7F212696338C30CD1407AF8ECB25610C39D6B00D4C43
SHA-512:	E99B7BA733C622C675AA7944338E994EE0D941663D812D702D986F4C162C4BC40FA2C837C6C761598B826A8CB7157DFBDDC20932B41B3D637209B3333BEEEB3
Malicious:	false
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0nf01gm5.vvm.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2br1q3bz.k2u.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2br1q3bz.k2u.psm1	
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_fgwq2vs1.fuu.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_kv2bxms5.otf.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_l1gqcsja.gw5.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_rhz4qu2t.ytv.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_rhz4qu2t.ytv.psm1	
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_udy30vs2.d4j.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_v2l21i0h.hu0.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_zm0bfdmr.3xj.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_zopv30bh.0qg.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\tmp2011.tmp	
Process:	C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1659
Entropy (8bit):	5.181728169538348
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB1tn:cbhH7MlNQ8/rydbz9I3YODOLNdq3V
MD5:	B27BCB69317043F17C0C452DBE3F9E4D
SHA1:	EF1FC850D6C2E7D02760122EF4DA4E8F918138A5
SHA-256:	1D46225432C74CBE4F42B1958FBEA7F1694B69FBFBE0F5FB9CB8043AB271554E
SHA-512:	216D3A4B522AB72A40D6F72A2FDB022324E91F286F2247B4A61AC8471235BFFE5ED8C7E6AFEC4019FB2ACD4EE2C5146CC162D9DC2B891300BA79B0F911629E 5
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>.. <StartWhenAv

C:\Users\user\AppData\Local\Temp\tmp864D.tmp	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1659
Entropy (8bit):	5.181728169538348
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB1tn:cbhH7MlNQ8/rydbz9I3YODOLNdq3V
MD5:	B27BCB69317043F17C0C452DBE3F9E4D
SHA1:	EF1FC850D6C2E7D02760122EF4DA4E8F918138A5
SHA-256:	1D46225432C74CBE4F42B1958FBEA7F1694B69FBFBE0F5FB9CB8043AB271554E
SHA-512:	216D3A4B522AB72A40D6F72A2FDB022324E91F286F2247B4A61AC8471235BFFE5ED8C7E6AFEC4019FB2ACD4EE2C5146CC162D9DC2B891300BA79B0F911629E 5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Roaming\AGYVBigGPY.exe	
Process:	C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	877568
Entropy (8bit):	7.25401903162754
Encrypted:	false
SSDEEP:	24576:0lO/1fBDLs8i4Y77/21nEgEcJCHwpKCfLc:0s/1pRY77/Lnc8HwlLc
MD5:	50AB414BE17F4E03BEE8F9C5CEE06335

C:\Users\user\AppData\Roaming\AGYVBigGPY.exe	
SHA1:	D0DEF6E40E7858A1B8C46D46F24A6B29499C7C37
SHA-256:	333B1AE9552E6A65AB7C4EDEE6677746E801EBED73294795B9057E17A0E284E6
SHA-512:	A397E7DCEF69FBD15A51080CA4F6AC2A698C9B880D0773950BD7C7777DFC2C5436A084694A825A60CD638E0B637599EE2C9A08119709FF62BBB89374A92361D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 24%, Browse • Antivirus: ReversingLabs, Detection: 48%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....`..... ... ...@....@.. ....@.....0 ..O....@..`]..... ..... ..H.....text..... ..... ..`.rsrc...`]...@...^.....@..@.rel oc.....b.....@..B.....d .....H.....T}..TI.....e.....Y.....(...*&..(!....*.s".....s#.....s$.....s%.....s&.....*...0.....~....o'....+..*.0..... .....~....o(....+..*.0.....~....o)....+..*.0.....~....o*....+..*.0.....~....o+....+..*.0..<.....~.....(,.....!r...p.....(-...o....s/.....~.....+..*.0.....~.....+..*"".....*.0..&.....(....r'.. p~....o0...(1.....t#....+..*...0..&.....(....r_..p~....o0...(1.....

C:\Users\user\AppData\Roaming\AGYVBigGPY.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe
File Type:	data
Category:	dropped
Size (bytes):	1624
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IlC0IlC0IlC0IlC0IlC08
MD5:	0D79388CEC6619D612C2088173BB6741
SHA1:	8A312E3198009C545D0CF3254572189D29A03EA7
SHA-256:	D7D423B23D932E306F3CCB2F7A984B7036A042C007A43FD655C6B57B960BB8DF
SHA-512:	53BB3E9263DFD746E7E8159466E220E6EC9D81E9D3F0E1D191E09CD511B7EB93B0BA65D13CE0C97C652ECD0F69BB991E6B1840F961BC65003C4DD7AA93EED 13
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.4056390622295662
Encrypted:	false
SSDEEP:	3:tvj:tvj
MD5:	02D5A593FEC6C4B98F90CCFF6ADD6E2C
SHA1:	F544B4D3B3717558E22E2B082BDD5018DE8AE765
SHA-256:	134D5CE17F0F33356C65007BB35715CC72F3A22E659E34F957212A7168BC1250
SHA-512:	3FEF07C755A48CA95F7559BB90FBF6AA858E44DDDE1D25A75AEEAF459980F5C656A52DA4F05C6E7BA788940FA49CA958B73E2B120BD1D24A48B9B4B0E47BBA 48
Malicious:	**true**
Preview:	...*J..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe
File Type:	data
Category:	modified
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYk:RzWDl3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F97
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYVsRLY6oRDT6P2bfVn1:RzWDlfRWDT621
MD5:	BB0F9B9992809E733EFFF8B0E562CFD6
SHA1:	F0BAB3CF73A04F5A689E6AFC764FEE9276992742
SHA-256:	C48F04FE7525AA3A3F9540889883F649726233DE021724823720A59B4F37CEAC
SHA-512:	AE4280AA460DC1C0301D458A3A443F6884A0BE37481737B2ADAFD72C33C55F09BED88ED239C91FE6F19CA137AC3CD7C9B8454C21D3F8E759687F701C8B3C7A6
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe
File Type:	data
Category:	dropped
Size (bytes):	426840
Entropy (8bit):	**7.999608491116724**
Encrypted:	**true**
SSDEEP:	12288:zKf137EiDsTjevgA4p0V7njXuWSvdVU7V4OC0Rr:+134i2lp67i5d8+OCg
MD5:	963D5E2C9C0008DFF05518B47C367A7F
SHA1:	C183D601FABBC9AC8FBFA0A0937DECC677535E74
SHA-256:	5EACF2974C9BB2C2E24CDC651C4840DD6F4B76A98F0E85E90279F1DBB2E6F3C0
SHA-512:	0C04E1C1A13070D48728D9F7F300D9B26DEC6EC8875D8D3017EAD52B9EE5BDF9B651A7F0FCC537761212831107646ED72B8ED017E7477E600BC0137EF857AE2
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^.._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m...RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=..:...L.g<.....I..%4[.G^.~.I'.....v.p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44Q?..N.....oX.A.....I...n?./.....$.!..;.^9"H.....*...OkF....v.m_.e.v..f...".bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&....g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=....{..J.1....2....<E{..<!G..

C:\Users\user\Documents\20210512\PowerShell_transcript.284992.8sAzw+Dk.20210512063128.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):	692
Entropy (8bit):	5.407987213876938
Encrypted:	false
SSDEEP:	12:57DtSA6NeidZO3fBd25orRx2DOzzUjjIneSuxNHwNeWo9Pw6jewGxMKjX4CIymgH:BxSACdZOvBdaUx2DOXUWeSuJWQHjeTKy
MD5:	3A634A38F704AF9AB4E9A667D92D3034
SHA1:	222A8C4D9E823EC6B241850C7CCF2974C0E61AF1
SHA-256:	E8B4E1ADB39E6C39FC0574DAF5EA61431B46E434BEF28A97198C5951C18C14E5
SHA-512:	91B54D26D21D2E6C418D94A4C768B75D36A1175DAE771C0A0C252446E807E99BD60EE5BBEADBB4AB0444D1956DE71F51FB6C54905EB67C9EADEC058A0673DDA
Malicious:	false

C:\Users\user\Documents\20210512\PowerShell_transcript.284992.8sAzw+Dk.20210512063128.txt	
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210512063235..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (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\AGYVBigGPY.exe..Process ID: 6644..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..**********..

C:\Users\user\Documents\20210512\PowerShell_transcript.284992.9Vv_x1G2.20210512063125.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):	690
Entropy (8bit):	5.387679237624884
Encrypted:	false
SSDEEP:	12:57DtSA6N6AidZO3fBd25orRx2DOzzUjjIneSur+WoCdPw6jewGxMKjX4CIymgSsx:BxSABAidZOvBdaUx2DOXUWeSur+WJdHy
MD5:	E259EFE2F9F722D8FAD8C2D100B4F7D8
SHA1:	249522ECDC08701B1AE06169CF01ABD96A6298F0
SHA-256:	3A0910F0E87A2AC0A3E168F00F39B1FA3AB1E24BA7FFCD715912DA0234BB013B
SHA-512:	0B94AEADE994A348C75DB5F8CD4781BEC9539FACF0C76C151BE6DE1955CAAC559B6B48330BABF1D31ED956CB30B895BC8FC75E54A6124A0E843130986D684177
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210512063243..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe..Process ID: 4708..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..**********..

C:\Users\user\Documents\20210512\PowerShell_transcript.284992.hO0k8c4M.20210512063049.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):	862
Entropy (8bit):	5.358854555611145
Encrypted:	false
SSDEEP:	24:BxSACydZOvBdaUx2DOXUWeSuJW8HjeTKKjX4CIym1ZJXguB:BZ8v6UoO+SP8qDYB1Z+g
MD5:	5A7EAF9BC9B5A1A7857562076DDD9A27
SHA1:	AF665A1EFAC71BAA8C9608C49E749232DA05547C
SHA-256:	29F03B82610592E81B95EC8B388AD6D71C2B9628278B70EECA20969667923FEB
SHA-512:	0B2BAA41EA3A6A42597EF0FAE72847ABF7350A899ABD17AA8E11AB3BFD406E9695FC4036B5051E6CEA42983B512632ED53BF4463140506D87DC008DB6BC9A42D
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210512063124..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (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\AGYVBigGPY.exe..Process ID: 5876..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: 20210512063125..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\AGYVBigGPY.exe..

C:\Users\user\Documents\20210512\PowerShell_transcript.284992.nr8pMLKJ.20210512063051.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):	862
Entropy (8bit):	5.350964262311637
Encrypted:	false
SSDEEP:	24:BxSA/dZOvBdaUx2DOXUWeSuJWrHjeTKKjX4CIym1ZJXjuB:BZqv6UoO+SPrqDYB1Z9g
MD5:	D6F00C73EE917223FE91D980F9E04494
SHA1:	2AF600781F3C4BB7BDBF700697F0B2446E563876
SHA-256:	48600FFDE10974E8E7F26EC3886BC216AE8F25608E3FD1EB572B3BB3F0FE82D0
SHA-512:	BB1714C33DD95C6215A85CA6BEE33D7EFE887592DDA183E0A1E6838D7484B72CAFDCDBBBF468B94649D8C854AFB941C3E2C3D4D296F7AA9BE327EF8D0CFD109
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210512063126..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (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\AGYVBigGPY.exe..Process ID: 2104..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: 20210512063126..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\AGYVBigGPY.exe..

C:\Users\user\Documents\20210512\PowerShell_transcript.284992.oeX3hsoM.20210512063048.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):	2071
Entropy (8bit):	5.327464690880742
Encrypted:	false
SSDEEP:	48:BZFv6UoO+SjXO5ezqDYB1Z3jXO50hZDv6UoO+SjXO5ezqDYB1ZGqA:BZp6UNlOeqDo1ZLO2hZz6UNlOeqDo1Z4
MD5:	A75C3AB8C2111C7C68CA9166B6B23C02
SHA1:	EF6FB863969049D9A608059A22B6DE1C676F7370
SHA-256:	F2835B9FF108B6C211CFC17B854E96141DBA2D96FDFEE3996DB69E78CBF59AA8
SHA-512:	14037BB575607BEC1F6782A5065ACD4A203F22582514B9D5AC4C15D62770998D6B259BF520D2FCBD1ED82FC9A54B38D0BA04A994A428CE9E9C36C8E397D3204
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210512063114..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe..Process ID: 5488..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: 20210512063115..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe..**********..Command start time: 20210512063915..**********..PS>Terminating

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.25401903162754
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Devizni izvod za partiju 0050100073053.exe
File size:	877568
MD5:	50ab414be17f4e03bee8f9c5cee06335
SHA1:	d0def6e40e7858a1b8c46d46f24a6b29499c7c37
SHA256:	333b1ae9552e6a65ab7c4edee6677746e801ebed73294795b9057e17a0e284e6
SHA512:	a397e7dcef69fbd15a51080ca4f6ac2a698c9b880d0773950bd7c7777dfc2c5436a084694a825a60cd638e0b637599ee2c9a08119709ff62bbb89374a92361dd
SSDEEP:	24576:0lO/1fBDLs8i4Y77/21nEgEcJCHwpKCfLc:0s/1pRY77/Lnc8HwlLc
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....`..... ... ...@....@.. .....@.....

File Icon

Icon Hash:	70d8ccd2d6ccf071

Static PE Info

General

Entrypoint:	0x4a2082
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT

General

Time Stamp:	0x6099070E [Mon May 10 10:12:30 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa2030	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa4000	0x35d60	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xda000	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	

Name	Virtual Address	Virtual Size	Is in Section
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	0xa0088	0xa0200	False	0.821009282299	data	7.66159215719	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa4000	0x35d60	0x35e00	False	0.368324934745	data	5.19988984772	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xda000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa42e0	0x94a9	PNG image data, 512 x 512, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xad78c	0x4872	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xb2000	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xc2828	0x94a8	data		
RT_ICON	0xcbcd0	0x5488	data		
RT_ICON	0xd1158	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 16318463, next used block 4294909696		
RT_ICON	0xd5380	0x25a8	data		
RT_ICON	0xd7928	0x10a8	data		
RT_ICON	0xd89d0	0x988	data		
RT_ICON	0xd9358	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xd97c0	0x92	data		
RT_VERSION	0xd9854	0x320	data		
RT_MANIFEST	0xd9b74	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

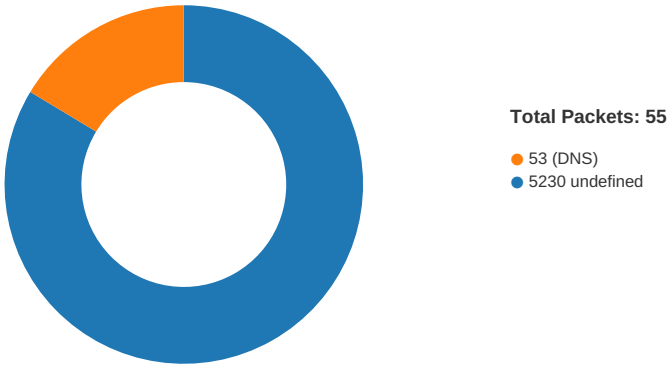
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	FXAssembly.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Geom3D
ProductVersion	1.0.0.0
FileDescription	GeometRi
OriginalFilename	FXAssembly.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-06:30:58.816182	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49715	5230	192.168.2.7	79.134.225.71
05/12/21-06:31:10.596014	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	5230	192.168.2.7	79.134.225.71
05/12/21-06:31:25.018858	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49723	5230	192.168.2.7	79.134.225.71
05/12/21-06:31:38.122656	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49725	5230	192.168.2.7	79.134.225.71
05/12/21-06:32:01.720351	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49726	5230	192.168.2.7	79.134.225.71
05/12/21-06:32:15.474221	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	5230	192.168.2.7	79.134.225.71
05/12/21-06:32:26.930999	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	5230	192.168.2.7	79.134.225.71
05/12/21-06:32:48.787980	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49730	5230	192.168.2.7	79.134.225.71

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 06:30:58.086821079 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:30:58.230679035 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:30:58.231053114 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:30:58.816181898 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:30:58.975986958 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:30:58.977135897 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:30:59.172842979 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:30:59.177062035 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:30:59.322546959 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:30:59.324124098 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:30:59.530989885 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:30:59.657485962 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:30:59.855797052 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:30:59.855914116 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.049459934 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.049767971 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.050853968 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.051115990 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.051256895 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.051403046 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.051767111 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.052685976 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.052742958 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.052867889 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.053277016 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.053433895 CEST	49715	5230	192.168.2.7	79.134.225.71

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 06:31:00.053596973 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.054292917 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.054467916 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.054598093 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.055284977 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.055593967 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.055622101 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.056200027 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.194266081 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.194540977 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.194603920 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.194674969 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.194694042 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.195782900 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.196319103 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.196455956 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.197699070 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.197850943 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.199152946 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.199263096 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.199323893 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.199448109 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.199470043 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.199474096 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.200005054 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.200119972 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.201483011 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.201638937 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.203311920 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.203594923 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.203903913 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.203922987 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.205699921 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.206407070 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.206943035 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.207770109 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.208364964 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.208719015 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.208739042 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.209036112 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.210536003 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.211755991 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.211779118 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.211838961 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.211843967 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.340907097 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.341697931 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.342142105 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.342258930 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.342504978 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.342662096 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.343385935 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.343470097 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.344639063 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.345073938 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.345360994 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.346088886 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.346431971 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.347409964 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.347713947 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.350450993 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.350615025 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.350811005 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.351110935 CEST	49715	5230	192.168.2.7	79.134.225.71

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 06:31:00.351134062 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.351718903 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.352113962 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.352211952 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.352830887 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.354094028 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.354219913 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.354240894 CEST	5230	49715	79.134.225.71	192.168.2.7
May 12, 2021 06:31:00.354324102 CEST	49715	5230	192.168.2.7	79.134.225.71
May 12, 2021 06:31:00.354338884 CEST	49715	5230	192.168.2.7	79.134.225.71

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 06:30:58.013586998 CEST	52816	53	192.168.2.7	8.8.4.4
May 12, 2021 06:30:58.072453976 CEST	53	52816	8.8.4.4	192.168.2.7
May 12, 2021 06:31:10.105428934 CEST	49958	53	192.168.2.7	8.8.4.4
May 12, 2021 06:31:10.165529966 CEST	53	49958	8.8.4.4	192.168.2.7
May 12, 2021 06:31:23.804364920 CEST	50452	53	192.168.2.7	8.8.4.4
May 12, 2021 06:31:23.863307953 CEST	53	50452	8.8.4.4	192.168.2.7
May 12, 2021 06:31:37.596846104 CEST	59730	53	192.168.2.7	8.8.4.4
May 12, 2021 06:31:37.656759024 CEST	53	59730	8.8.4.4	192.168.2.7
May 12, 2021 06:31:57.780992985 CEST	51919	53	192.168.2.7	8.8.4.4
May 12, 2021 06:31:57.839382887 CEST	53	51919	8.8.4.4	192.168.2.7
May 12, 2021 06:32:13.039374113 CEST	64296	53	192.168.2.7	8.8.4.4
May 12, 2021 06:32:13.099052906 CEST	53	64296	8.8.4.4	192.168.2.7
May 12, 2021 06:32:26.642617941 CEST	56680	53	192.168.2.7	8.8.4.4
May 12, 2021 06:32:26.701777935 CEST	53	56680	8.8.4.4	192.168.2.7
May 12, 2021 06:32:37.803754091 CEST	58820	53	192.168.2.7	8.8.4.4
May 12, 2021 06:32:37.860908031 CEST	53	58820	8.8.4.4	192.168.2.7
May 12, 2021 06:32:48.533617973 CEST	60983	53	192.168.2.7	8.8.4.4
May 12, 2021 06:32:48.590641975 CEST	53	60983	8.8.4.4	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 06:30:58.013586998 CEST	192.168.2.7	8.8.4.4	0x4092	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 06:31:10.105428934 CEST	192.168.2.7	8.8.4.4	0x8a62	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 06:31:23.804364920 CEST	192.168.2.7	8.8.4.4	0x70a9	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 06:31:37.596846104 CEST	192.168.2.7	8.8.4.4	0x3e7a	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 06:31:57.780992985 CEST	192.168.2.7	8.8.4.4	0x188f	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 06:32:13.039374113 CEST	192.168.2.7	8.8.4.4	0xc160	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 06:32:26.642617941 CEST	192.168.2.7	8.8.4.4	0xef36	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 06:32:37.803754091 CEST	192.168.2.7	8.8.4.4	0x7e6e	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 06:32:48.533617973 CEST	192.168.2.7	8.8.4.4	0xfb75	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

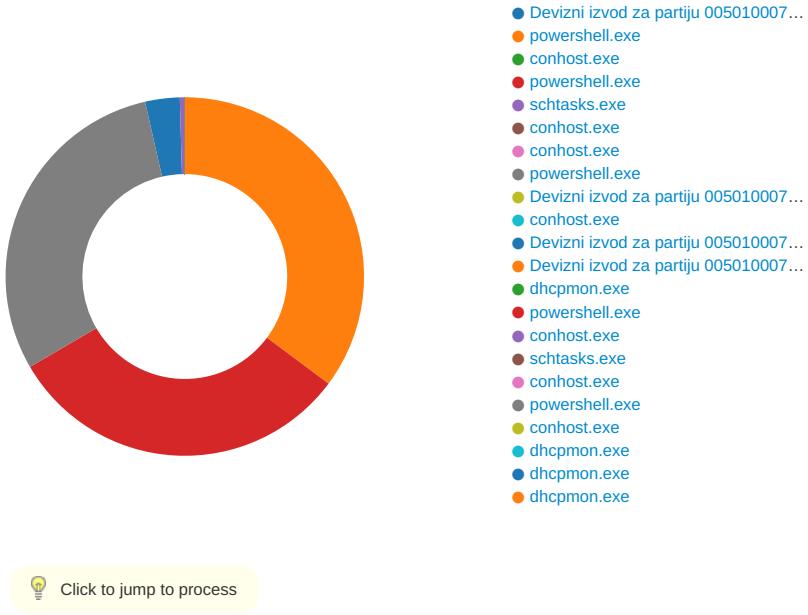
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 06:30:58.072453976 CEST	8.8.4.4	192.168.2.7	0x4092	No error (0)	emedoo.ddns.net		79.134.225.71	A (IP address)	IN (0x0001)
May 12, 2021 06:31:10.165529966 CEST	8.8.4.4	192.168.2.7	0x8a62	No error (0)	emedoo.ddns.net		79.134.225.71	A (IP address)	IN (0x0001)
May 12, 2021 06:31:23.863307953 CEST	8.8.4.4	192.168.2.7	0x70a9	No error (0)	emedoo.ddns.net		79.134.225.71	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 06:31:37.656759024 CEST	8.8.4.4	192.168.2.7	0x3e7a	No error (0)	emedoo.ddns.net		79.134.225.71	A (IP address)	IN (0x0001)
May 12, 2021 06:31:57.839382887 CEST	8.8.4.4	192.168.2.7	0x188f	No error (0)	emedoo.ddns.net		79.134.225.71	A (IP address)	IN (0x0001)
May 12, 2021 06:32:13.099052906 CEST	8.8.4.4	192.168.2.7	0xc160	No error (0)	emedoo.ddns.net		79.134.225.71	A (IP address)	IN (0x0001)
May 12, 2021 06:32:26.701777935 CEST	8.8.4.4	192.168.2.7	0xef36	No error (0)	emedoo.ddns.net		79.134.225.71	A (IP address)	IN (0x0001)
May 12, 2021 06:32:37.860908031 CEST	8.8.4.4	192.168.2.7	0x7e6e	No error (0)	emedoo.ddns.net		79.134.225.71	A (IP address)	IN (0x0001)
May 12, 2021 06:32:48.590641975 CEST	8.8.4.4	192.168.2.7	0xfb75	No error (0)	emedoo.ddns.net		79.134.225.71	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Devizni izvod za partiju 0050100073053.exe PID: 4504 Parent PID: 5716

General

Start time:	06:30:43
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe'
Imagebase:	0x260000

File size:	877568 bytes
MD5 hash:	50AB414BE17F4E03BEE8F9C5CEE06335
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: 00000002.00000002.255288442.0000000002A3B000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.256690894.0000000003A11000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.256690894.0000000003A11000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.256690894.0000000003A11000.00000004.00000001.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	724660AC	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	724660AC	unknown
C:\Users\user\AppData\Roaming\AGYVBigGPY.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	24D03D4	CopyFileW
C:\Users\user\AppData\Roaming\AGYVBigGPY.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	24D03D4	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2011.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	24D0AE0	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Devizni izvod za partiju 0050100073053.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	724534A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2011.tmp	success or wait	1	24D0F56	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\AGYVBigGPY.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 0e 07 99 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 02 0a 00 00 60 03 00 00 00 00 00 82 20 0a 00 00 20 00 00 00 40 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 0d 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......`.......... ....P......`....... ... ...@....@.. ....@................	success or wait	4	24D03D4	CopyFileW
C:\Users\user\AppData\Roaming\ AGYVBigGPY.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	24D03D4	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2011.tmp	unknown	1659	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 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 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	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </Registrati	success or wait	1	24D0D6F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Devizni izvod za partiju 0050100073053.exe.log	unknown	525	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 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	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\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7273A33A	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	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile

Analysis Process: powershell.exe PID: 5488 Parent PID: 4504

General

Start time:	06:30:45
Start date:	12/05/2021
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\Devizni izvod za partiju 0050100073053.exe'
Imagebase:	0x1110000
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

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	6CEFCF06	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	6CEFCF06	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	6BCA5B28	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	6BCA5B28	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_v2l21i0h.hu0.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BD41E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_udy30vs2.d4j.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BD41E60	CreateFileW
C:\Users\user\Documents\20210512	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BD4BEFF	CreateDirectoryW
C:\Users\user\Documents\20210512\PowerShell_transcript.284992.oeX3hsoM.20210512063048.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BD41E60	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	3	6BD41E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_v2l21i0h.hu0.ps1	success or wait	1	6BD46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_udy30vs2.d4j.psm1	success or wait	1	6BD46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_v2l21i0h.hu0.ps1	unknown	1	31	1	success or wait	1	6BD41B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_udy30vs2.d4j.psm1	unknown	1	31	1	success or wait	1	6BD41B4F	WriteFile
C:\Users\user\Documents\20210512\PowerShell_transcript.284992.oeX3hsoM.20210512063048.txt	unknown	3	ef bb bf	...	success or wait	1	6BD41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210512\PowerShell_transcript.284992.oeX3hsoM.20210512063048.txt	unknown	709	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 31 32 30 36 33 31 31 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 66 72 6f 6e 74 64 65 73 6b 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 66 72 6f 6e 74 64 65 73 6b 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 32 38 34 39 39 32 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f	**********..Windows PowerShell transcript start..Start time: 20210512063114..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (Microsoft Windows NT 10.0.17134.0)..Host Applicatio	success or wait	15	6BD41B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....w.e....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	3	6BD41B4F	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 0d 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	2	6BD41B4F	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	2	6BD41B4F	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	6BD41B4F	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	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CED5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CED5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CED5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CE303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CEDCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CEDCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CEDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CE303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CED5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CE303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CED5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CED5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6CEE1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21320	success or wait	1	6CEE203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CE303DE	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	6BD41B4F	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	6BD41B4F	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	6BD41B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	126	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BD41B4F	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	6CE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CE303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	2	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	72	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6BD41B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management .Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	6CEBD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management .Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	6CEBD72F	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	8	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	6BD41B4F	ReadFile

Analysis Process: conhost.exe PID: 5304 Parent PID: 5488

General

Start time:	06:30:46
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 5876 Parent PID: 4504

General

Start time:	06:30:46
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -Ex clusionPath 'C:\Users\user\AppData\Roaming\AGYVBigGPY.exe'
Imagebase:	0x1110000
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

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	6CEFCF06	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	6CEFCF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_0nf01gm5.vvm.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BD41E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_l1gqcsja.gw5.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BD41E60	CreateFileW
C:\Users\user\Documents\20210512\PowerShell_transcript.284992.hO0k8c4M.20210512063049.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BD41E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_0nf01gm5.vvm.ps1	success or wait	1	6BD46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_l1gqcsja.gw5.psm1	success or wait	1	6BD46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_0nf01gm5.vvm.ps1	unknown	1	31	1	success or wait	1	6BD41B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_l1gqcsja.gw5.psm1	unknown	1	31	1	success or wait	1	6BD41B4F	WriteFile
C:\Users\user\Documents\20210512\PowerShell_transcript.284992.hO0k8c4M.20210512063049.txt	unknown	3	ef bb bf	...	success or wait	1	6BD41B4F	WriteFile
C:\Users\user\Documents\20210512\PowerShell_transcript.284992.hO0k8c4M.20210512063049.txt	unknown	689	2a 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 31 32 30 36 33 31 32 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 66 72 6f 6e 74 64 65 73 6b 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 66 72 6f 6e 74 64 65 73 6b 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 32 38 34 39 39 32 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f	**********..Windows PowerShell transcript start..Start time: 20210512063124..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (Microsoft Windows NT 10.0.17134.0)..Host Applicatio	success or wait	5	6BD41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	698	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 02 00 00 00 f8 77 dc 65 ca 9f d5 08 61 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5c 31 2e 30 2e 30 2e 31 5c 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 2e 70 73 64 31 0d 00 00 00 11 00 00 00 53 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 18 00 00 00 55 6e 72 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 0f 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 0c 00 00 00 53 61 76 65 2d 50 61 63 6b 61 67 65 08 00 00	PSMODULECACHE.....we....a...C:\Program Files (x86)\Windows PowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package...	success or wait	3	6BD41B4F	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 0d 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	2	6BD41B4F	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	2	6BD41B4F	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	6BD41B4F	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	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CED5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CED5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CED5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CE303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CEDCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CEDCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CEDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CE303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CED5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CE303DE	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	6CE303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CED5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6CED5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CED5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6CEE1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21320	success or wait	1	6CEE203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CE303DE	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	6BD41B4F	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	6BD41B4F	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	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	2	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	115	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BD41B4F	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	6CE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CE303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	8	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	2	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	59	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\ MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6BD41B4F	ReadFile

Analysis Process: schtasks.exe PID: 1744 Parent PID: 4504

General

Start time:	06:30:46
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\AGYVBigGPY' /XML 'C:\Users\user\AppData\Local\Temp\tmp2011.tmp'
Imagebase:	0xbe0000
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\tmp2011.tmp	unknown	2	success or wait	1	BEAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2011.tmp	unknown	1660	success or wait	1	BEABD9	ReadFile

Analysis Process: conhost.exe PID: 2148 Parent PID: 5876

General

Start time:	06:30:46
Start date:	12/05/2021

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: conhost.exe PID: 5852 Parent PID: 1744

General

Start time:	06:30:47
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 2104 Parent PID: 4504

General

Start time:	06:30:47
Start date:	12/05/2021
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\AGYVBigGPY.exe'
Imagebase:	0x1110000
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	6CEFCF06	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	6CEFCF06	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	6BCA5B28	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	6BCA5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fgwq2vs1.fuu.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BD41E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rhz4qu2t.ytv.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BD41E60	CreateFileW
C:\Users\user\Documents\20210512\PowerShell_transcript.284992.nr8pMLKJ.20210512063051.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BD41E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fgwq2vs1.fuu.ps1	success or wait	1	6BD46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rhz4qu2t.ytv.psm1	success or wait	1	6BD46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fgwq2vs1.fuu.ps1	unknown	1	31	1	success or wait	1	6BD41B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rhz4qu2t.ytv.psm1	unknown	1	31	1	success or wait	1	6BD41B4F	WriteFile
C:\Users\user\Documents\20210512\PowerShell_transcript.284992.nr8pMLKJ.20210512063051.txt	unknown	3	ef bb bf	...	success or wait	1	6BD41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210512\PowerShell_transcript.284992.nr8pMLKJ.20210512063051.txt	unknown	689	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 31 32 30 36 33 31 32 36 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 66 72 6f 6e 74 64 65 73 6b 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 66 72 6f 6e 74 64 65 73 6b 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 32 38 34 39 39 32 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f	********************..Windows PowerShell transcript start..Start time: 20210512063126..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (Microsoft Windows NT 10.0.17134.0)..Host Applicatio	success or wait	5	6BD41B4F	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 0d 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)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	2	6BD41B4F	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	2	6BD41B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2242	2d 41 70 70 4c 6f 63 6b 65 72 50 6f 6c 69 63 79 08 00 00 00 13 00 00 00 4e 65 77 2d 41 70 70 4c 6f 63 6b 65 72 50 6f 6c 69 63 79 08 00 00 00 13 00 00 00 47 65 74 2d 41 70 70 4c 6f 63 6b 65 72 50 6f 6c 69 63 79 08 00 00 00 1c 00 00 00 47 65 74 2d 41 70 70 4c 6f 63 6b 65 72 46 69 6c 65 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 00 00 00 00 79 48 e2 38 ca 9f d5 08 49 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 65 73 74 65 72 5c 33 2e 34 2e 30 5c 50 65 73 74 65 72 2e 70 73 64 31 17 00 00 00 08 00 00 00 44 65 73 63 72 69 62 65 02 00 00 00 11 00 00 00 47 65 74 2d 54 65 73 74 44 72 69 76 65 49 74 65 6d 02 00 00 00 0b 00 00 00 4e 65 77 2d 46 69 78	-AppLockerPolicy.....New-AppLockerPolicy.....Get-AppLockerPolicy.....Get-AppLockerFileInformation.....yH.8.....I...C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fix	success or wait	2	6BD41B4F	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	6BD41B4F	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	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CED5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CED5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CED5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CE303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CEDCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CEDCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CEDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CE303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CED5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CE303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CED5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CED5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6CEE1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21320	success or wait	1	6CEE203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CE303DE	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	6BD41B4F	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	6BD41B4F	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	6BD41B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	137	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6BD41B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BD41B4F	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	6CE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CE303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CE303DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BD41B4F	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	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	2	6BD41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	2	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CED5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	53	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6BD41B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6BD41B4F	ReadFile

Analysis Process: Devizni izvod za partiju 0050100073053.exe PID: 5932 Parent PID: 4504

General

Start time:	06:30:48
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe
Imagebase:	0x2a0000
File size:	877568 bytes

MD5 hash:	50AB414BE17F4E03BEE8F9C5CEE06335
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: conhost.exe PID: 5340 Parent PID: 2104

General

Start time:	06:30:48
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: Devizni izvod za partiju 0050100073053.exe PID: 6164 Parent PID: 4504

General

Start time:	06:30:49
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe
Imagebase:	0x430000
File size:	877568 bytes
MD5 hash:	50AB414BE17F4E03BEE8F9C5CEE06335
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Devizni izvod za partiju 0050100073053.exe PID: 6196 Parent PID: 4504

General

Start time:	06:30:50
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Devizni izvod za partiju 0050100073053.exe
Imagebase:	0x580000
File size:	877568 bytes
MD5 hash:	50AB414BE17F4E03BEE8F9C5CEE06335
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:

0000000D.00000003.296886935.0000000004040000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000D.00000003.296886935.0000000004040000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.541194418.0000000003D8D000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.546573646.00000000056B0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.546573646.00000000056B0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.546573646.00000000056B0000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.552591050.0000000006A50000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.552591050.0000000006A50000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.546929623.0000000005950000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.546929623.0000000005950000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.503765658.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.503765658.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.503765658.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.546313038.00000000055C0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.546313038.00000000055C0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000003.297630594.000000000410E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000D.00000003.297630594.000000000410E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.551440197.0000000006890000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.551440197.0000000006890000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.552438629.0000000006A20000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.552438629.0000000006A20000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.546995313.00000000059E0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.546995313.00000000059E0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.551688994.00000000068C0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.551688994.00000000068C0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000003.297298308.0000000004098000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000D.00000003.297298308.0000000004098000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.551733160.00000000068D0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.551733160.00000000068D0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.551056353.0000000006730000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.551056353.0000000006730000.00000004.00000001.sdmp, Author:

	Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.547173286.0000000005A80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.547173286.0000000005A80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.546044032.0000000005580000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.546044032.0000000005580000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.546082364.0000000005590000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.546082364.0000000005590000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.535153965.0000000002D8C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.545285946.00000000053A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.545285946.00000000053A0000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	low

Analysis Process: dhcpmon.exe PID: 6792 Parent PID: 3292

General

Start time:	06:31:07
Start date:	12/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xeb0000
File size:	877568 bytes
MD5 hash:	50AB414BE17F4E03BEE8F9C5CEE06335
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.373412048.0000000004761000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.373412048.0000000004761000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.373412048.0000000004761000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000013.00000002.364891578.000000000378B000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.383604898.000000000525A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.383604898.000000000525A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.383604898.000000000525A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 24%, Metadefender, Browse • Detection: 48%, ReversingLabs
Reputation:	low

Analysis Process: powershell.exe PID: 4708 Parent PID: 6792

General

Start time:	06:31:14
Start date:	12/05/2021
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:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 6076 Parent PID: 4708

General

Start time:	06:31:15
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 6092 Parent PID: 6792

General

Start time:	06:31:15
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\AGYVBigGPY' /XML 'C:\Users\user\AppData\Local\Temp\tmp864D.tmp'
Imagebase:	0xd90000
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: 4428 Parent PID: 6092

General

Start time:	06:31:15
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6644 Parent PID: 6792

General

Start time:	06:31:17
Start date:	12/05/2021
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\AGYVBigGPY.exe'
Imagebase:	0x1110000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 1880 Parent PID: 6644

General

Start time:	06:31:18
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 4608 Parent PID: 6792

General

Start time:	06:31:18
Start date:	12/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x140000
File size:	877568 bytes
MD5 hash:	50AB414BE17F4E03BEE8F9C5CEE06335
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 5356 Parent PID: 6792

General

Start time:	06:31:23
Start date:	12/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x3c0000
File size:	877568 bytes
MD5 hash:	50AB414BE17F4E03BEE8F9C5CEE06335
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 900 Parent PID: 6792

General

Start time:	06:31:26
Start date:	12/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x600000
File size:	877568 bytes
MD5 hash:	50AB414BE17F4E03BEE8F9C5CEE06335
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: 00000022.00000002.383744500.0000000003EC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000022.00000002.383744500.0000000003EC1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000022.00000002.357286802.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000022.00000002.357286802.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000022.00000002.357286802.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

Code Analysis