

JOE Sandbox Cloud BASIC



**ID:** 402568

**Sample Name:** transfer pdf.exe

**Cookbook:** default.jbs

**Time:** 09:34:22

**Date:** 03/05/2021

**Version:** 32.0.0 Black Diamond

# Table of Contents

Table of Contents	2
Analysis Report transfer pdf.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Threatname: NanoCore	4
Yara Overview	5
Memory Dumps	5
Unpacked PEs	5
Sigma Overview	5
System Summary:	6
Signature Overview	6
AV Detection:	6
Networking:	6
E-Banking Fraud:	6
System Summary:	6
Data Obfuscation:	6
Boot Survival:	6
Hooking and other Techniques for Hiding and Protection:	6
Malware Analysis System Evasion:	7
HIPS / PFW / Operating System Protection Evasion:	7
Stealing of Sensitive Information:	7
Remote Access Functionality:	7
Mitre Att&ck Matrix	7
Behavior Graph	7
Screenshots	8
Thumbnails	8
Antivirus, Machine Learning and Genetic Malware Detection	9
Initial Sample	9
Dropped Files	9
Unpacked PE Files	9
Domains	9
URLs	9
Domains and IPs	10
Contacted Domains	10
Contacted URLs	10
URLs from Memory and Binaries	10
Contacted IPs	11
Public	11
General Information	11
Simulations	12
Behavior and APIs	12
Joe Sandbox View / Context	12
IPs	12
Domains	12
ASN	12
JA3 Fingerprints	13
Dropped Files	13
Created / dropped Files	13
Static File Info	18
General	18
File Icon	18

<b>Static PE Info</b>	<b>18</b>
General	18
Entrypoint Preview	19
Data Directories	20
Sections	21
Resources	21
Imports	21
Version Infos	21
<b>Network Behavior</b>	<b>21</b>
Snort IDS Alerts	21
TCP Packets	22
<b>Code Manipulations</b>	<b>23</b>
<b>Statistics</b>	<b>23</b>
Behavior	24
<b>System Behavior</b>	<b>24</b>
<b>Analysis Process: transfer pdf.exe PID: 5984 Parent PID: 5684</b>	<b>24</b>
General	24
File Activities	24
File Created	24
File Deleted	25
File Written	25
File Read	26
<b>Analysis Process: powershell.exe PID: 4012 Parent PID: 5984</b>	<b>27</b>
General	27
File Activities	27
File Created	27
File Deleted	28
File Written	28
File Read	31
<b>Analysis Process: conhost.exe PID: 452 Parent PID: 4012</b>	<b>34</b>
General	34
<b>Analysis Process: powershell.exe PID: 3060 Parent PID: 5984</b>	<b>34</b>
General	34
File Activities	35
File Created	35
File Deleted	35
File Written	35
File Read	39
<b>Analysis Process: schtasks.exe PID: 5316 Parent PID: 5984</b>	<b>42</b>
General	42
File Activities	42
File Read	42
<b>Analysis Process: conhost.exe PID: 1140 Parent PID: 3060</b>	<b>42</b>
General	42
<b>Analysis Process: conhost.exe PID: 6152 Parent PID: 5316</b>	<b>43</b>
General	43
<b>Analysis Process: powershell.exe PID: 6272 Parent PID: 5984</b>	<b>43</b>
General	43
File Activities	43
File Created	43
File Deleted	44
File Written	44
File Read	47
<b>Analysis Process: conhost.exe PID: 6288 Parent PID: 6272</b>	<b>50</b>
General	50
<b>Analysis Process: transfer pdf.exe PID: 6296 Parent PID: 5984</b>	<b>50</b>
General	50
<b>Disassembly</b>	<b>52</b>
Code Analysis	52

# Analysis Report transfer pdf.exe

## Overview

### General Information

Sample Name:	transfer pdf.exe
Analysis ID:	402568
MD5:	ceab5875bc8300..
SHA1:	7f181a1500e1b2c.
SHA256:	56f803925d37e48.
Tags:	exe NanoCore RAT
Infos:	
Most interesting Screenshot:	

### Detection

**MALICIOUS**

SUSPICIOUS

CLEAN

UNKNOWN

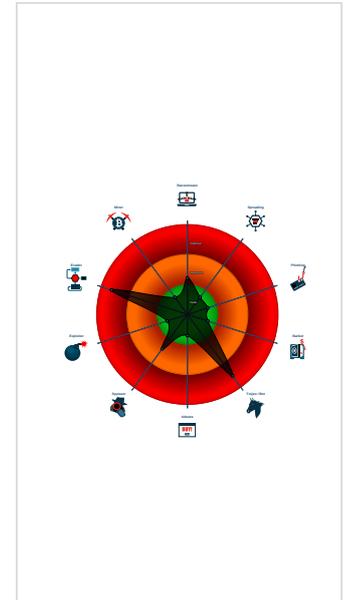
**Nanocore**

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

### Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through ...)
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file...
- Snort IDS alert for network traffic (e...
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia...
- Adds a directory exclusion to Windo...
- C2 URLs / IPs found in malware con...
- Hides that the sample has been dow...
- Tries to detect sandboxes and other...
- Uses schtasks.exe or at.exe to add ...
- Activates or Modifies Learning date...

### Classification



## Startup

- System is w10x64
- transfer pdf.exe (PID: 5984 cmdline: 'C:\Users\user\Desktop\transfer pdf.exe' MD5: CEAB5875BC8300BADE1FA862D446AF5B)
  - powershell.exe (PID: 4012 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\transfer pdf.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 452 cmdline: 'C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 3060 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\mrCqHfpog.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1140 cmdline: 'C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5316 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\mrCqHfpog' /XML 'C:\Users\user\AppData\Local\Temp\tmp1C2B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6152 cmdline: 'C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6272 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\mrCqHfpog.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6288 cmdline: 'C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - transfer pdf.exe (PID: 6296 cmdline: 'C:\Users\user\Desktop\transfer pdf.exe' MD5: CEAB5875BC8300BADE1FA862D446AF5B)
- cleanup

## Malware Configuration

Threatname: NanoCore

```

{
  "Version": "1.2.2.0",
  "Mutex": "97a824b7-e666-4a22-b2e3-fb501d91",
  "Group": "king",
  "Domain1": "23.105.131.171",
  "Domain2": "",
  "Port": 4040,
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}

```

## Yara Overview

### Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.513751941.000000000599 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	<ul style="list-style-type: none"> <li>0xf7ad:\$x1: NanoCore.ClientPluginHost</li> <li>0xf7da:\$x2: IClientNetworkHost</li> </ul>
0000000C.00000002.513751941.000000000599 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	<ul style="list-style-type: none"> <li>0xf7ad:\$x2: NanoCore.ClientPluginHost</li> <li>0x10888:\$s4: PipeCreated</li> <li>0xf7c7:\$s5: IClientLoggingHost</li> </ul>
0000000C.00000002.513751941.000000000599 0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000C.00000002.515591721.0000000006D9 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	<ul style="list-style-type: none"> <li>0x1f1db:\$x1: NanoCore.ClientPluginHost</li> <li>0x1f1f5:\$x2: IClientNetworkHost</li> </ul>
0000000C.00000002.515591721.0000000006D9 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	<ul style="list-style-type: none"> <li>0x1f1db:\$x2: NanoCore.ClientPluginHost</li> <li>0x22518:\$s4: PipeCreated</li> <li>0x1f1c8:\$s5: IClientLoggingHost</li> </ul>

[Click to see the 45 entries](#)

### Unpacked PE's

Source	Rule	Description	Author	Strings
12.2.transfer pdf.exe.6d40000.34.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	<ul style="list-style-type: none"> <li>0x59eb:\$x1: NanoCore.ClientPluginHost</li> <li>0x5b48:\$x2: IClientNetworkHost</li> </ul>
12.2.transfer pdf.exe.6d40000.34.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	<ul style="list-style-type: none"> <li>0x59eb:\$x2: NanoCore.ClientPluginHost</li> <li>0x6941:\$s3: PipeExists</li> <li>0x5be1:\$s4: PipeCreated</li> <li>0x5a05:\$s5: IClientLoggingHost</li> </ul>
12.2.transfer pdf.exe.44ce7b8.9.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	<ul style="list-style-type: none"> <li>0xd9ad:\$x1: NanoCore.ClientPluginHost</li> <li>0xd9da:\$x2: IClientNetworkHost</li> </ul>
12.2.transfer pdf.exe.44ce7b8.9.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	<ul style="list-style-type: none"> <li>0xd9ad:\$x2: NanoCore.ClientPluginHost</li> <li>0xea88:\$s4: PipeCreated</li> <li>0xd9c7:\$s5: IClientLoggingHost</li> </ul>
12.2.transfer pdf.exe.44ce7b8.9.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

[Click to see the 147 entries](#)

## Sigma Overview

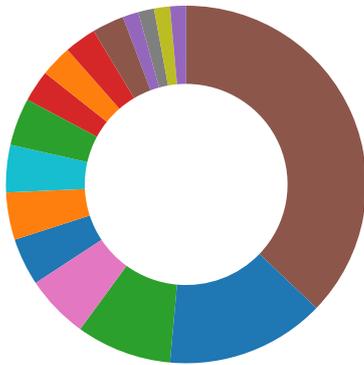
## System Summary:



Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

## Signature Overview



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

Click to jump to signature section

## AV Detection:



Found malware configuration

Yara detected Nanocore RAT

## Networking:



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

C2 URLs / IPs found in malware configuration

## E-Banking Fraud:



Yara detected Nanocore RAT

## System Summary:



Malicious sample detected (through community Yara rule)

## Data Obfuscation:



.NET source code contains potential unpacker

## Boot Survival:



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

## Hooking and other Techniques for Hiding and Protection:



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

## Malware Analysis System Evasion:



Yara detected AntiVM3

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

## HIPS / PFW / Operating System Protection Evasion:



Adds a directory exclusion to Windows Defender

## Stealing of Sensitive Information:



Yara detected Nanocore RAT

## Remote Access Functionality:



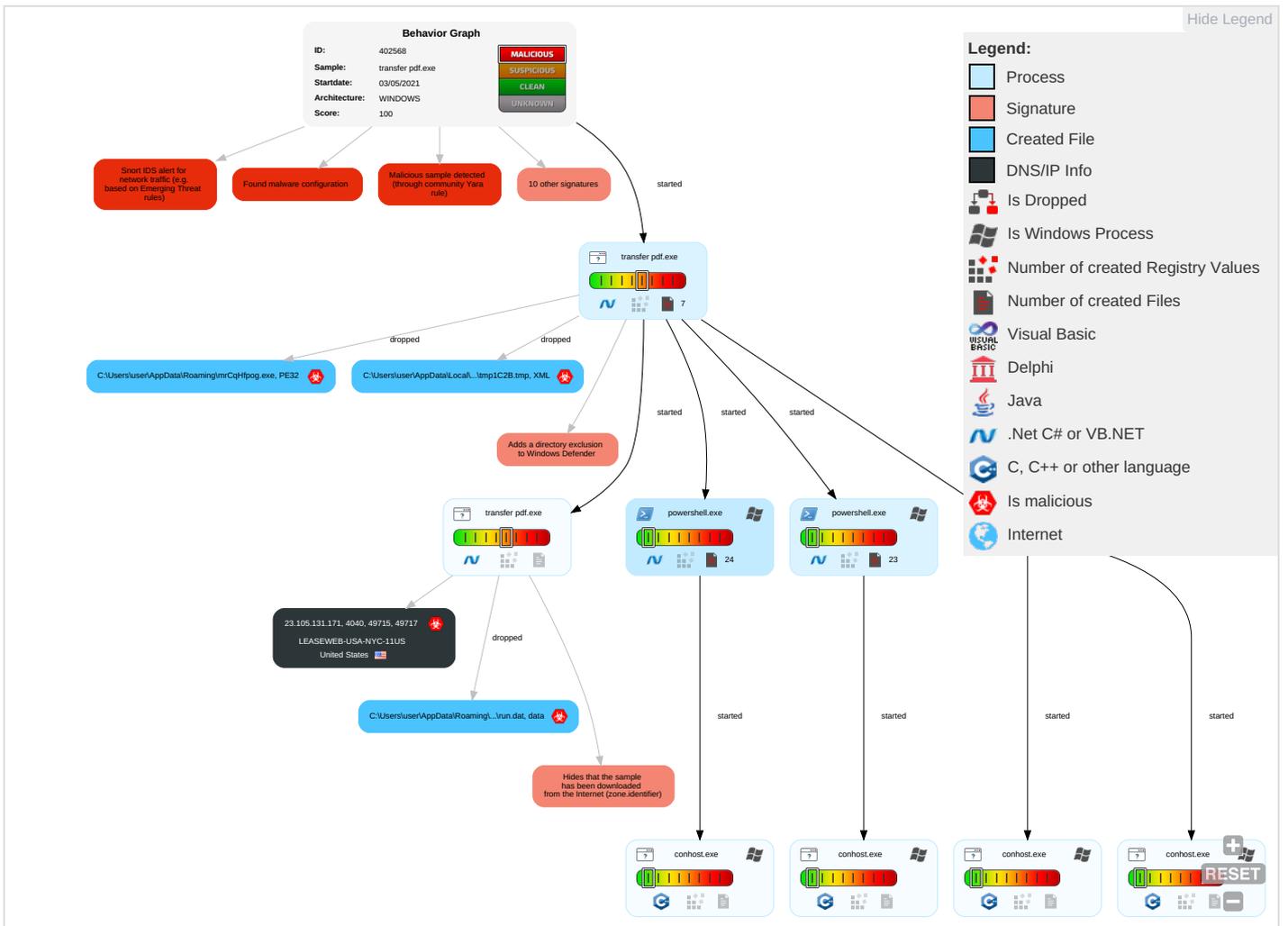
Detected Nanocore Rat

Yara detected Nanocore RAT

## Mitre Att&ck Matrix

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

## Behavior Graph



## Screenshots

### Thumbnails

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





## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

No Antivirus matches

### Dropped Files

No Antivirus matches

### Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.transfer pdf.exe.5990000.25.unpack	100%	Avira	TR/NanoCore.fadte		<a href="#">Download File</a>
12.2.transfer pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		<a href="#">Download File</a>

### Domains

No Antivirus matches

### URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
23.105.131.171	1%	Virusotal		<a href="#">Browse</a>
23.105.131.171	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://crl.microsoft.co	0%	URL Reputation	safe	
http://crl.microsoft.co	0%	URL Reputation	safe	
http://crl.microsoft.co	0%	URL Reputation	safe	
http://crl.microsoft.co	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.microH	0%	Avira URL Cloud	safe	
http://crl.micr	0%	URL Reputation	safe	
http://crl.micr	0%	URL Reputation	safe	
http://crl.micr	0%	URL Reputation	safe	
http://crl.micr	0%	URL Reputation	safe	

## Domains and IPs

### Contacted Domains

No contacted domains info

### Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	low
23.105.131.171	true	<ul style="list-style-type: none"> <li>1%, Virustotal, <a href="#">Browse</a></li> <li>Avira URL Cloud: safe</li> </ul>	unknown

### URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000003.0000002.421231170.00000000468D000.00000004.00000001.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000003.0000002.421231170.00000000468D000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000003.0000002.421231170.00000000468D000.00000004.00000001.sdmp, powershell.exe, 0000000A.00000003.84164451.00000000798A000.00000004.00000001.sdmp	false		high
http://crl.microsoft.co	powershell.exe, 00000006.0000003.383513280.000000009369000.00000004.00000001.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	unknown
http://https://go.micro	powershell.exe, 00000006.0000003.370559526.00000000519A000.00000004.00000001.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	unknown
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000003.0000002.421231170.00000000468D000.00000004.00000001.sdmp	false		high
http://https://go.microH	powershell.exe, 00000003.0000003.361194913.000000004EF5000.00000004.00000001.sdmp	false	<ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>	unknown
http://crl.micr	powershell.exe, 00000006.0000003.383513280.000000009369000.00000004.00000001.sdmp	false	<ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul>	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	transfer pdf.exe, 00000001.0000002.268177444.0000000002D91000.00000004.00000001.sdmp, powershell.exe, 00000003.00000002.419297952.0000000004551000.0000004.00000001.sdmp	false		high
http://https://github.com/unguest	transfer pdf.exe	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000003.00000002.421231170.000000000468D000.00000004.00000001.sdmp, powershell.exe, 0000000A.00000003.384164451.000000000798A000.00000004.00000001.sdmp	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	transfer pdf.exe, 00000001.0000002.268883772.0000000002DE4000.00000004.00000001.sdmp	false		high
http://https://github.com/unguest9WinForms_RecursiveFormCreate5WinForms_SeelInnerExceptionGProperty	transfer pdf.exe	false		high

## Contacted IPs



## Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.105.131.171	unknown	United States		396362	LEASEWEB-USA-NYC-11US	true

## General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	402568
Start date:	03.05.2021
Start time:	09:34:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 24s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	transfer pdf.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:	35
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:	<ul style="list-style-type: none"> <li>• HCA enabled</li> <li>• EGA enabled</li> <li>• HDC enabled</li> <li>• AMSI enabled</li> </ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@15/21@0/1
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"> <li>• Successful, ratio: 0.3% (good quality ratio 0.2%)</li> <li>• Quality average: 50.2%</li> <li>• Quality standard deviation: 29.6%</li> </ul>
HCA Information:	<ul style="list-style-type: none"> <li>• Successful, ratio: 98%</li> <li>• Number of executed functions: 0</li> <li>• Number of non-executed functions: 0</li> </ul>
Cookbook Comments:	<ul style="list-style-type: none"> <li>• Adjust boot time</li> <li>• Enable AMSI</li> <li>• Found application associated with file extension: .exe</li> </ul>
Warnings:	<p>Show All</p> <ul style="list-style-type: none"> <li>• Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.</li> <li>• TCP Packets have been reduced to 100</li> <li>• Report size exceeded maximum capacity and may have missing behavior information.</li> <li>• Report size getting too big, too many NtOpenKeyEx calls found.</li> <li>• Report size getting too big, too many NtProtectVirtualMemory calls found.</li> <li>• Report size getting too big, too many NtQueryValueKey calls found.</li> </ul>

## Simulations

### Behavior and APIs

Time	Type	Description
09:35:12	API Interceptor	959x Sleep call for process: transfer pdf.exe modified
09:36:03	API Interceptor	169x Sleep call for process: powershell.exe modified

## Joe Sandbox View / Context

### IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.105.131.171	DHLAWB# 9284880911 pdf.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	

### Domains

No context

### ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LEASEWEB-USA-NYC-11US	DHLAWB# 9284880911.pdf.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.171
	PO.pdf.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.190
	PO.pdf.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.161
	PO.pdf.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.161
	SecuritelInfo.com.Trojan.Win32.Save.a.29244.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.161
	ZBgnuLqtOd.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.161
	ZE9u48l6N4.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.161
	PO copy.pdf.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.161
	invoice&packing list.pdf.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.161
	PO.PDF.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.161
	PO copy.pdf.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.161
	Ordem urgente AWB674653783- FF2453.PDF.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.132
	Remittance FormDoc.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.19.227.243
	Presupuesto de orden urgente KTX88467638.pdf.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.132
	Dringende Bestellung Zitat CTX88467638.pdf.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.132
	shipping document.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.207
	6V9espP5wD.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.195
	NVAbIqNO9h.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.209
	UUGCfhIdFD.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.228
	KPcrOQcb5P.exe	<a href="#">Get hash</a>	malicious	<a href="#">Browse</a>	• 23.105.131.228

### JA3 Fingerprints

No context

### Dropped Files

No context

### Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\transfer.pdf.exe.log	
Process:	C:\Users\user\Desktop\transfer.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHkOzAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBV0GlpN6KQkj2Wkj4iUxtaKdROdBLNxp5nYoGib4J:cBV3lpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DED83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Reputation:	moderate, very likely benign file
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-Scr- pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... .....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22288
Entropy (8bit):	5.602814793744318
Encrypted:	false
SSDEEP:	384:VtCD+0oDonJQYSBKniultlo8i7Y9gNSJUeRS1BMrmc71AV7YbUWnT64l+rqq;DonD4Kiultp82NXexh+klL3
MD5:	92A779066F9EE92202EEF43F55A54EA
SHA1:	744752178D8549B017C08F8D17F0CB12ECF308BA
SHA-256:	FF11401D3FD9BA987DD1AAB644EF22FBE29887FF9A66B4AD172F0E8FB260A8A5
SHA-512:	1AE78AB47A4D22B86401F1A157E494D7192AAF0EC6B3A1D37C164D642A10CA4C1CB500E1F71A71888A1711FFEA82F9219AC8D486621C50ACED492CB41E0163F0
Malicious:	false
Preview:	@...e..... .....h.8.....@.....H.....<@.^L."My...P.... Microsoft.PowerShell.ConsoleHostD.....fZve...F...x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o..A...4B.....System..4.....Zg5...O..g..q.....System.Xml.L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....L.}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management..4.....].D.E...#.....System.Data.H.....H..m)jUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>.m.....Sy stem.Transactions.<.....):gK..G..\$.1.q.....System.ConfigurationP...../C..J..%..].....%Microsoft.PowerShell.Commands.Utility..D.....-D.F.<.;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\_PSScriptPolicyTest_0gnanrsx.mye.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651C
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\_PSScriptPolicyTest_hysdr11b.k4x.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651C
Malicious:	false
Preview:	1

<b>C:\Users\user\AppData\Local\Temp\_PSScriptPolicyTest_ ndu5cgvr.co5.psm1</b>	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

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

<b>C:\Users\user\AppData\Local\Temp\_PSScriptPolicyTest_ptwdp50q.rjn.ps1</b>	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

<b>C:\Users\user\AppData\Local\Temp\_PSScriptPolicyTest_yeec2spy.ean.ps1</b>	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1





<b>C:\Users\user\Documents\20210503\PowerShell_transcript.724471.OeTIOZLu.20210503093522.txt</b>	
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):	5795
Entropy (8bit):	5.390124498744504
Encrypted:	false
SSDEEP:	96:BZu/5NqPqDo1Z6qpZp/5NqPqDo1ZvyoajZd/5NqPqDo1ZbHqq7ZA:Cc
MD5:	59B521E8FBB02BE927BF8E01F289B150
SHA1:	2D9FFDAD88942468FA1CFBCFE5915F6B441E037A
SHA-256:	483CF0EF5BBF8EE1DA99D0859A8D2C68C048D9E6840CFEDDF934137F164E003C
SHA-512:	A07AF1F5436FE202229936C19155DA9BDE04550B8D17B0093D081163F2A23D51EA6D6CDF7BFEC86564689FE1C6EAD245E2FF312930431C308C7D4236945372B5
Malicious:	false
Preview:	<pre> ***** .Windows PowerShell transcript start..Start time: 20210503093551..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 724471 (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\mrCqHfpog.exe..Process ID: 3060..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: 20210503093551..***** ..PS&gt;Add-MpPreference -ExclusionPath C:\Users\user\AppData \Roaming\mrCqHfpog.exe..***** .Windows PowerShell transcript start..Start time: 20210503094241..Username: computer\user..RunAs User: computer\ </pre>

## Static File Info

<b>General</b>	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.9250591786965385
TrID:	<ul style="list-style-type: none"> <li>Win32 Executable (generic) Net Framework (10011505/4) 49.80%</li> <li>Win32 Executable (generic) a (10002005/4) 49.75%</li> <li>Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%</li> <li>Windows Screen Saver (13104/52) 0.07%</li> <li>Generic Win/DOS Executable (2004/3) 0.01%</li> </ul>
File name:	transfer pdf.exe
File size:	768000
MD5:	ceab5875bc8300bade1fa862d446af5b
SHA1:	7f181a1500e1b2cbf7c76466210c58d166c30c62
SHA256:	56f803925d37e489e72c9e3a7bf128d46fd29b62f858961b2f644edf09530602
SHA512:	1eabe540d9a60c4bfcda210fc2172602cc5e1f4e5bf51cde1b8357ed150c18105fcd7c780f02b24d0e53ada213fc15ce609ed6a0f2dad23f6d9794af2cd447
SSDEEP:	12288:YHybHxkWZyccgdFi7YuybPUMHMevVw4vPPQW83vMj:YI+WZyLcgdlTmUDkVwePYW8fl
File Content Preview:	<pre> MZ.....@.....!..L!Th is program cannot be run in DOS mode...\$.....PE..L.../ . ....P.....@.. @..... </pre>

## File Icon

Icon Hash:	00828e8e8686b000

## Static PE Info

<b>General</b>	
Entrypoint:	0x4bc2e6
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:	0x608FA02F [Mon May 3 07:03:11 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

## Entrypoint Preview

### Instruction

jmp dword ptr [00402000h]

add byte ptr [eax], al



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	0xba2ec	0xba400	False	0.940277632131	data	7.93274067684	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbe000	0xeb0	0x1000	False	0.371826171875	data	4.73728210413	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc0000	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_VERSION	0xbe090	0x384	data		
RT_MANIFEST	0xbe424	0xa85	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

## Imports

DLL	Import
mSCOREE.dll	_CorExeMain

## Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	ConsoleKeyInfo.exe
FileVersion	1.0.1.35
CompanyName	Unguest
LegalTrademarks	Unguest
Comments	A light media player
ProductName	LightWatch
ProductVersion	1.0.1.35
FileDescription	LightWatch
OriginalFilename	ConsoleKeyInfo.exe

## Network Behavior

### Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-09:35:32.623530	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49715	4040	192.168.2.5	23.105.131.171
05/03/21-09:35:39.337049	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49717	4040	192.168.2.5	23.105.131.171
05/03/21-09:35:46.986072	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	4040	192.168.2.5	23.105.131.171
05/03/21-09:35:53.895415	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	4040	192.168.2.5	23.105.131.171
05/03/21-09:36:00.948328	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49723	4040	192.168.2.5	23.105.131.171
05/03/21-09:36:07.255510	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49725	4040	192.168.2.5	23.105.131.171
05/03/21-09:36:14.135768	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49726	4040	192.168.2.5	23.105.131.171
05/03/21-09:36:21.266663	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	4040	192.168.2.5	23.105.131.171

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-09:36:28.213344	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49730	4040	192.168.2.5	23.105.131.171
05/03/21-09:36:35.225006	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	4040	192.168.2.5	23.105.131.171
05/03/21-09:36:42.377921	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	4040	192.168.2.5	23.105.131.171
05/03/21-09:36:49.360959	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	4040	192.168.2.5	23.105.131.171
05/03/21-09:36:56.440801	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49739	4040	192.168.2.5	23.105.131.171
05/03/21-09:37:03.419217	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	4040	192.168.2.5	23.105.131.171
05/03/21-09:37:10.430106	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	4040	192.168.2.5	23.105.131.171
05/03/21-09:37:17.389616	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	4040	192.168.2.5	23.105.131.171

## TCP Packets

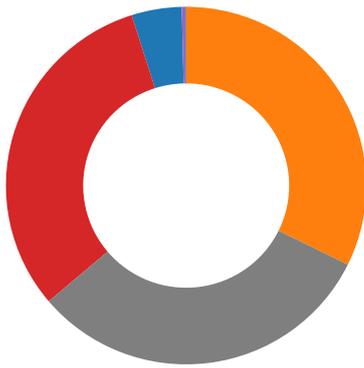
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 09:35:32.085064888 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:32.431684017 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:32.431962013 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:32.623529911 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:32.974828005 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:32.975075006 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:33.360786915 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:33.362013102 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:33.698458910 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:33.725450993 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.101778030 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.101877928 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.504880905 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.513500929 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.514358997 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.515269041 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.515669107 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.516179085 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.516285896 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.517843962 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.518191099 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.518256903 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.519788027 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.519870996 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.519959927 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.520190954 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.521356106 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.521500111 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.893935919 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.901930094 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.901961088 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.902031898 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.905492067 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.905528069 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.905611992 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.908291101 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.908400059 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.909270048 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.909370899 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.910259962 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.910916090 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.911220074 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.911292076 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.912779093 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.912916899 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.914225101 CEST	4040	49715	23.105.131.171	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 09:35:34.915096045 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.918266058 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.918410063 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.920197010 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.921345949 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.921459913 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.922826052 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.923165083 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.923265934 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.925879002 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.925983906 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.926775932 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.926966906 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.928792000 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.929321051 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.929414034 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:34.930727005 CEST	4040	49715	23.105.131.171	192.168.2.5
May 3, 2021 09:35:34.930850029 CEST	49715	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:39.011243105 CEST	49717	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:39.335288048 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:39.336292982 CEST	49717	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:39.337049007 CEST	49717	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:39.680708885 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:39.681143045 CEST	49717	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:40.019908905 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:40.021090984 CEST	49717	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:40.396903992 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:40.397041082 CEST	49717	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:40.795402050 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:40.796209097 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:40.796314001 CEST	49717	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:40.796452045 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:40.797306061 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:40.797887087 CEST	49717	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:40.798741102 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:40.799690008 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:40.799784899 CEST	49717	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:40.799844027 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:40.801011086 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:40.801323891 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:40.801430941 CEST	49717	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:40.801465034 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:40.801568031 CEST	49717	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:41.003602982 CEST	49717	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:41.127368927 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:41.128123999 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:41.128245115 CEST	49717	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:41.130992889 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:41.131089926 CEST	49717	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:41.131705046 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:41.132095098 CEST	49717	4040	192.168.2.5	23.105.131.171
May 3, 2021 09:35:41.137669086 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:41.138117075 CEST	4040	49717	23.105.131.171	192.168.2.5
May 3, 2021 09:35:41.138274908 CEST	49717	4040	192.168.2.5	23.105.131.171

## Code Manipulations

## Statistics

## Behavior



- transfer pdf.exe
- powershell.exe
- conhost.exe
- powershell.exe
- schtasks.exe
- conhost.exe
- conhost.exe
- powershell.exe
- conhost.exe
- transfer pdf.exe

 Click to jump to process

## System Behavior

**Analysis Process: transfer pdf.exe PID: 5984 Parent PID: 5684**

### General

Start time:	09:35:10
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\transfer pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\transfer pdf.exe'
Imagebase:	0x810000
File size:	768000 bytes
MD5 hash:	CEAB5875BC8300BADE1FA862D446AF5B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	<ul style="list-style-type: none"> <li>● Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.272783114.0000000003D99000.00000004.00000001.sdmp, Author: Florian Roth</li> <li>● Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.272783114.0000000003D99000.00000004.00000001.sdmp, Author: Joe Security</li> <li>● Rule: NanoCore, Description: unknown, Source: 00000001.00000002.272783114.0000000003D99000.00000004.00000001.sdmp, Author: Kevin Breen &lt;kevin@techanarchy.net&gt;</li> <li>● Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.268883772.0000000002DE4000.00000004.00000001.sdmp, Author: Joe Security</li> </ul>
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	6DB0CF06	unknown



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1C2B.tmp	unknown	1646	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.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>.. </RegistrationI	success or wait	1	6C951B4F	WriteFile
C:\Users\user\AppData\Local\Mi crosoft\CLR_v4.0.32\UsageLogs\transfer pdf.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 4e 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0.1,"Win RT", "NotApp",1..2,"Microsoft.Vi sualBasic, Version=10.0.0.0, Cult ure=neutral, PublicKeyToken=b0 3f5f7f11d50a3a",0..2,"Syst em.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyTok en=b77a5c561934e089",0. .3,"System, Version=4.	success or wait	1	6DE1C907	WriteFile

#### File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152 fe02a317a7aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAECA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C951B4F	ReadFile

### Analysis Process: powershell.exe PID: 4012 Parent PID: 5984

#### General

Start time:	09:35:18
Start date:	03/05/2021
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\transfer pdf.exe'
Imagebase:	0x380000
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	6DB0CF06	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	6DB0CF06	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	6C8B5B28	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	6C8B5B28	unknown
C:\Users\user\AppData\Local\Temp\_PSscriptPolicyTest_nwtmaqkg.cxx.ps1	read attributes   synchronize   generic write	device	sequential only   synchronous io non alert   non directory file   open no recall	success or wait	1	6C951E60	CreateFileW



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\Power ShellG et1.0.0.1\PowerShellGet.p sd1.....Uninstall- Module..... .inmo.....fimo.....Install- Module.....New-scr iptFileInfo.....Publish- Module.....Install-Sc	success or wait	2	6C951B4F	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.Utilit y\Microsoft.PowerShell.Utility. psd1m.....Remove- Variable.....Convert- String.....Trace- Command.....Sort- Object.....Register- ObjectEvent.....Get- Runspace.....Format- Table.....Wait- Debugger.....Get- Runspace	success or wait	2	6C951B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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	-	success or wait	2	6C951B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff 95 ce 12 09 ca 9f d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e.....Install- PackageProvid er.....Import- PackageProvider.....Get- PackageProvider. .....Register- PackageSource. .....Uninstall-Package..... ..Find- PackageProvider..... .....I...C:\Windows\system3 2\WindowsPowerShell\v1. 0\Modules\Defender\Def	success or wait	1	6C951B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 10 00 00 00 e9 12 00 00 15 00 00 00 ea 0d ea 05 00 08 ef 07 c8 07 00 00 00 00 aa 02 3e 00 c9 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e..... .....>.....@.....	success or wait	1	6DDD76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 3a 00 00 00 0e 00 20 00	H.....<@.^...L."My.. :.....	success or wait	16	6DDD76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	16	6DDD76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	10	6DDD76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	10	6DDD76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 54 01 40 00 f9 3e 40 01 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 ed 44 00 01 6d 45 00 01 45 4d 00 01 dc 71 00 01 dd 71 00 01 f8 53 00 01 98 25 00 01 ba 6e 00 01 34 26 00 01 35 26 00 01 37 26 00	..... T.@..>@...@.V.@.H .@.X.@. [.@.NT@.HT@..S@..S@. hT@..S @..S@..S@.\.@..T@..T@. @X@.?X@. .T@..S@..S@..T@..T@.x T@.zT@..T @.=M@.DM@.:M@."M@. M@.!M@.;M@. .D@..D@.@M@. <M@.\$M@.8M..?M..BM ...D..mE..EM...q...S...%. ..n..4&..5&..7&.	success or wait	10	6DDD76FC	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	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAECA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAE5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DAF1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21312	success or wait	1	6DAF203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA403DE	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	6C951B4F	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	6C951B4F	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	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	127	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf496405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb2e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown



File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C951B4F	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	6DACD72F	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	6DACD72F	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C951B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6C951B4F	ReadFile

### Analysis Process: conhost.exe PID: 452 Parent PID: 4012

#### General

Start time:	09:35:18
Start date:	03/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

### Analysis Process: powershell.exe PID: 3060 Parent PID: 5984

#### General

Start time:	09:35:18
Start date:	03/05/2021
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\mrCqHfpg.exe'
Imagebase:	0x380000
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:\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	6C8B5B28	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	6C8B5B28	unknown
C:\Users\user	read data or list directory   synchronize	device	directory file   synchronous io non alert   open for backup ident   open reparse point	object name collision	1	6DB0CF06	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	6DB0CF06	unknown
C:\Users\user\AppData\Local\Temp\_PSscriptPolicyTest_yeec2spy.ean.ps1	read attributes   synchronize   generic write	device	sequential only   synchronous io non alert   non directory file   open no recall	success or wait	1	6C951E60	CreateFileW
C:\Users\user\AppData\Local\Temp\_PSscriptPolicyTest_ndu5cgv. co5.psm1	read attributes   synchronize   generic write	device	sequential only   synchronous io non alert   non directory file   open no recall	success or wait	1	6C951E60	CreateFileW
C:\Users\user\Documents\20210503\PowerShell_transcript.724471.OeTIOZLu.20210503093522.txt	read attributes   synchronize   generic read   generic write	device	synchronous io non alert   non directory file   open no recall	success or wait	1	6C951E60	CreateFileW

#### File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\_PSscriptPolicyTest_yeec2spy.ean.ps1	success or wait	1	6C956A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\_PSscriptPolicyTest_ndu5cgv. co5.psm1	success or wait	1	6C956A95	DeleteFileW

#### File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\_PSscriptPolicyTest_yeec2spy.ean.ps1	unknown	1	31	1	success or wait	1	6C951B4F	WriteFile
C:\Users\user\AppData\Local\Temp\_PSscriptPolicyTest_ndu5cgv. co5.psm1	unknown	1	31	1	success or wait	1	6C951B4F	WriteFile
C:\Users\user\Documents\20210503\PowerShell_transcript.724471.OeTIOZLu.20210503093522.txt	unknown	3	ef bb bf	...	success or wait	1	6C951B4F	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.UtilityM icrosoft.PowerShell.Utility. psd1m.....Remove- Variable.....Convert- String.....Trace- Command.....Sort- Object.....Register- ObjectEvent.....Get- Runspace.....Format- Table.....Wait- Debugger.....Get- Runspac	success or wait	1	6C951B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff 95 ce 12 09 ca 9f d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e.....Install- PackageProvid er.....Import- PackageProvider.....Get- PackageProvider. .....Register- PackageSource. .....Uninstall-Package..... ..Find- PackageProvider..... .....I...C:\Windows\system3 2\WindowsPowerShell\v1. 0\Modules\Defender\Def	success or wait	1	6C951B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2446	10 00 00 00 52 65 73 75 6d 65 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 1c 00 00 00 42 61 63 6b 75 70 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 25 00 00 00 53 68 6f 77 2d 42 69 74 4c 6f 63 6b 65 72 52 65 71 75 69 72 65 64 41 63 74 69 6f 6e 73 49 6e 74 65 72 6e 61 6c 02 00 00 00 17 00 00 00 55 6e 6c 6f 63 6b 2d 50 61 73 73 77 6f 72 64 49 6e 74 65 72 6e 61 6c 02 00 00 00 10 00 00 00 55 6e 6c 6f 63 6b 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 18 00 00 00 41 64 64 2d 54 70 6d 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 25 00 00 00 41 64 64 2d 52 65 63 6f 76 65 72 79 50 61 73 73 77 6f 72 64 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 55 6e 6c 6f 63 6b 2d 52 65 63 6f 76 65 72	....Resume- BitLocker.....Backup- BitLockerKeyProtector.... %...Show- BitLockerRequiredActi onsInternal.....Unlock- Pass wordInternal.....Unlock- BitLocker.....Add- TpmProtector Internal...%...Add- RecoveryPa sswordProtectorInternal.... ...Unlock-Recover	success or wait	1	6C951B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 88 14 00 00 18 00 00 00 ea 0d 51 04 99 09 89 09 69 09 00 00 00 00 4f 03 4d 00 c9 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00	@...e.....Q... ..i.....O.M.....@.....	success or wait	1	6DDD76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 52 00 00 00 0e 00 20 00	H.....<@.^...L."My.. .:R.....	success or wait	17	6DDD76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.Cons oleHost	success or wait	17	6DDD76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6DDD76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6DDD76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 54 01 40 00 f9 3e 40 01 ce 67 40 01 99 01 40 00 fb 00 40 00 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 16 3b 40 01 45 4d 40 01 dc 71 40 01 dd 71 40 01 42 4d 00 01 ed 44 00 01 6d 45 00 01 f8 53 40 01 98 25 40	.....T.@..>@..g@...@... @...@.V.@.H.@.X.@. [.@.NT@.HT@..S @..S@.hT@..S@..S@..S @.\.@..T@..T@.@X@?. X@..T@..S@..S@..T@..T @.xT@.zT@..T@.=M@.D M@.:M@."M@. M@.!M@.;M@..D@..D@. @M@.<M@.\$M@.8M@.?. M@.:@.EM@..q@..q@.B M...D..mE...S@..%@	success or wait	11	6DDD76FC	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	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorliba152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAECA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a6ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAE5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DAF1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21312	success or wait	1	6DAF203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\18d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA403DE	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	6C951B4F	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	6C951B4F	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	6C951B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	135	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mif49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\1b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\18d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C951B4F	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	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShellModuleAnalysisCache	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShellModuleAnalysisCache	unknown	62	success or wait	1	6C951B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShellModuleAnalysisCache	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	10	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C951B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C951B4F	ReadFile

### Analysis Process: schtasks.exe PID: 5316 Parent PID: 5984

#### General

Start time:	09:35:19
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\mrCqHfpog' /XML 'C:\Users\user\AppData\Local\Temp\tmp1C2B.tmp'
Imagebase:	0x860000
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\tmp1C2B.tmp	unknown	2	success or wait	1	86AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1C2B.tmp	unknown	1647	success or wait	1	86ABD9	ReadFile

### Analysis Process: conhost.exe PID: 1140 Parent PID: 3060

#### General

Start time:	09:35:19
Start date:	03/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff797770000
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: 6152 Parent PID: 5316**

**General**

Start time:	09:35:19
Start date:	03/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

**Analysis Process: powershell.exe PID: 6272 Parent PID: 5984**

**General**

Start time:	09:35:20
Start date:	03/05/2021
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\mrCqHfpg.exe'
Imagebase:	0x380000
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:\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	6C8B5B28	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	6C8B5B28	unknown
C:\Users\user	read data or list directory   synchronize	device	directory file   synchronous io non alert   open for backup ident   open reparse point	object name collision	1	6DB0CF06	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	6DB0CF06	unknown



File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE..... <.e...Y...C:\Program Files (x86)\Windows PowerShell\Modules\Power ShellG et1.0.0.1\PowerShellGet.p sd1.....Uninstall- Module..... .inmo.....fimo.....Install- Module.....New-scr iptFileInfo.....Publish- Module.....Install-Sc	success or wait	1	6C951B4F	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.Utilit y\Microsoft.PowerShell.Utility. psd1m.....Remove- Variable.....Convert- String.....Trace- Command.....Sort- Object.....Register- ObjectEvent.....Get- Runspace.....Format- Table.....Wait- Debugger.....Get- Runspace	success or wait	1	6C951B4F	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- PackageProvid er.....Import- PackageProvider.....Get- PackageProvider. .....Register- PackageSource. .....Uninstall-Package..... ..Find- PackageProvider..... .....I...C:\Windows\sysste m3 2\WindowsPowerShell\v1. 0\Modules\Defender\Def	success or wait	1	6C951B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2446	10 00 00 00 52 65 73 75 6d 65 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 1c 00 00 00 42 61 63 6b 75 70 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 25 00 00 00 53 68 6f 77 2d 42 69 74 4c 6f 63 6b 65 72 52 65 71 75 69 72 65 64 41 63 74 69 6f 6e 73 49 6e 74 65 72 6e 61 6c 02 00 00 00 17 00 00 00 55 6e 6c 6f 63 6b 2d 50 61 73 73 77 6f 72 64 49 6e 74 65 72 6e 61 6c 02 00 00 00 10 00 00 00 55 6e 6c 6f 63 6b 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 18 00 00 00 41 64 64 2d 54 70 6d 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 25 00 00 00 41 64 64 2d 52 65 63 6f 76 65 72 79 50 61 73 73 77 6f 72 64 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 55 6e 6c 6f 63 6b 2d 52 65 63 6f 76 65 72	....Resume- BitLocker.....Backup- BitLockerKeyProtector.... %...Show- BitLockerRequiredActi onsInternal.....Unlock- Pass wordInternal.....Unlock- BitLocker.....Add- TpmProtector Internal....%...Add- RecoveryPa sswordProtectorInternal..... ...Unlock-Recover	success or wait	1	6C951B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 7c 14 00 00 19 00 00 00 ea 0d f5 04 f5 08 e1 08 c1 08 00 00 00 00 68 02 38 00 c9 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e..... ..... .....h.8.....@.....	success or wait	1	6DDD76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 50 00 00 00 0e 00 20 00	H.....<@.^...L."My.. :P.....	success or wait	17	6DDD76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.Cons oleHost	success or wait	17	6DDD76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6DDD76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6DDD76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 54 01 40 00 f9 3e 40 01 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 00 01 78 54 00 01 7a 54 00 01 95 54 00 01 3d 4d 00 01 44 4d 00 01 3a 4d 00 01 22 4d 00 01 20 4d 00 01 21 4d 00 01 3b 4d 00 01 e0 44 00 01 e5 44 00 01 40 4d 00 01 3c 4d 00 01 24 4d 00 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 ed 44 00 01 6d 45 00 01 45 4d 00 01 dc 71 00 01 dd 71 00 01 f8 53 00 01 98 25 00 01 ba 6e 00 01 34 26 00 01 35 26 00 01 37 26 00	..... .....T.@..>@...@.V.@.H .@.X.@. [.@.NT@.HT@..S@..S@. hT@..S @..S@..S@.\.@..T@..T@. @X@.?X@. .T@..S@..S@..T@..T@..XT.. zT...T..=M..DM..M..M.. M..M..M..D..D..@M.. <M..\$M..8M..?M..BM.. ...D.mE..EM...q...S...%.. ..n.4&..5&..7&.	success or wait	11	6DDD76FC	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	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DAE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DA403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAECA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DAE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DAE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DAE5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DAF1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21312	success or wait	1	6DAF203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA403DE	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	6C951B4F	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	6C951B4F	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	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	129	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C951B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb2e6\System.ni.dll.aux	unknown	620	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DA403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DA403DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DAE5705	unknown



File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C951B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C951B4F	ReadFile

### Analysis Process: conhost.exe PID: 6288 Parent PID: 6272

#### General

Start time:	09:35:20
Start date:	03/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

### Analysis Process: transfer pdf.exe PID: 6296 Parent PID: 5984

#### General

Start time:	09:35:20
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\transfer pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\transfer pdf.exe
Imagebase:	0xe10000
File size:	768000 bytes
MD5 hash:	CEAB5875BC8300BADE1FA862D446AF5B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	<ul style="list-style-type: none"> <li>Rule: Nanocore_RAT_Gen_2, Description: Detects the Nanocore RAT, Source: 000000C.0000002.513751941.000000005990000.0000004.0000001.sdmp, Author: Florian Roth</li> <li>Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 000000C.0000002.513751941.000000005990000.0000004.0000001.sdmp, Author:</li> </ul>

Florian Roth

- Rule: JoeSecurity\_Nanocore, Description: Yara detected Nanocore RAT, Source: 000000C.00000002.513751941.0000000005990000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore\_RAT\_Gen\_2, Description: Detets the Nanocore RAT, Source: 000000C.00000002.515591721.0000000006D90000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Feb18\_1, Description: Detects Nanocore RAT, Source: 000000C.00000002.515591721.0000000006D90000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Gen\_2, Description: Detets the Nanocore RAT, Source: 000000C.00000002.515333490.0000000006D10000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Feb18\_1, Description: Detects Nanocore RAT, Source: 000000C.00000002.515333490.0000000006D10000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Gen\_2, Description: Detets the Nanocore RAT, Source: 000000C.00000002.501766215.00000000015F0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Feb18\_1, Description: Detects Nanocore RAT, Source: 000000C.00000002.501766215.00000000015F0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Gen\_2, Description: Detets the Nanocore RAT, Source: 000000C.00000002.515124476.0000000006A60000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Feb18\_1, Description: Detects Nanocore RAT, Source: 000000C.00000002.515124476.0000000006A60000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Gen\_2, Description: Detets the Nanocore RAT, Source: 000000C.00000002.515475125.0000000006D50000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Feb18\_1, Description: Detects Nanocore RAT, Source: 000000C.00000002.515475125.0000000006D50000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity\_Nanocore, Description: Yara detected Nanocore RAT, Source: 000000C.00000002.512261589.0000000004D53000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 000000C.00000002.512261589.0000000004D53000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@technarchy.net>
- Rule: Nanocore\_RAT\_Gen\_2, Description: Detets the Nanocore RAT, Source: 000000C.00000002.515442936.0000000006D40000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Feb18\_1, Description: Detects Nanocore RAT, Source: 000000C.00000002.515442936.0000000006D40000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Gen\_2, Description: Detets the Nanocore RAT, Source: 000000C.00000002.515411177.0000000006D30000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Feb18\_1, Description: Detects Nanocore RAT, Source: 000000C.00000002.515411177.0000000006D30000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity\_Nanocore, Description: Yara detected Nanocore RAT, Source: 000000C.00000002.512487196.0000000004EB4000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 000000C.00000002.512487196.0000000004EB4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@technarchy.net>
- Rule: Nanocore\_RAT\_Gen\_2, Description: Detets the Nanocore RAT, Source: 000000C.00000002.494628444.0000000004020000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity\_Nanocore, Description: Yara detected Nanocore RAT, Source: 000000C.00000002.494628444.0000000004020000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 000000C.00000002.494628444.0000000004020000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@technarchy.net>
- Rule: Nanocore\_RAT\_Gen\_2, Description: Detets the Nanocore RAT, Source: 000000C.00000002.515674870.0000000006DD0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Feb18\_1, Description: Detects Nanocore RAT, Source: 000000C.00000002.515674870.0000000006DD0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity\_Nanocore, Description: Yara detected Nanocore RAT, Source: 000000C.00000002.511981202.0000000004B6A000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 000000C.00000002.511981202.0000000004B6A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@technarchy.net>
- Rule: NanoCore, Description: unknown, Source: 000000C.00000002.509710048.0000000003646000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@technarchy.net>
- Rule: NanoCore, Description: unknown, Source: 000000C.00000002.512384046.0000000004DC9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@technarchy.net>
- Rule: Nanocore\_RAT\_Gen\_2, Description: Detets the Nanocore RAT, Source: 000000C.00000002.515504174.0000000006D60000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Feb18\_1, Description: Detects Nanocore RAT, Source: 000000C.00000002.515504174.0000000006D60000.00000004.00000001.sdmp, Author: Florian Roth

- Rule: JoeSecurity\_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.510709014.00000000044C9000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.510709014.00000000044C9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore\_RAT\_Gen\_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.515369623.0000000006D20000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Feb18\_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.515369623.0000000006D20000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Gen\_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.515060286.0000000006A30000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Feb18\_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.515060286.0000000006A30000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Gen\_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.513626328.0000000005930000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Feb18\_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.513626328.0000000005930000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Gen\_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.515563891.0000000006D80000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore\_RAT\_Feb18\_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.515563891.0000000006D80000.00000004.00000001.sdmp, Author: Florian Roth

Reputation:

low

## Disassembly

## Code Analysis