ID: 882707
Sample Name: file.exe
Cookbook: default.jbs
Time: 17:17:17
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

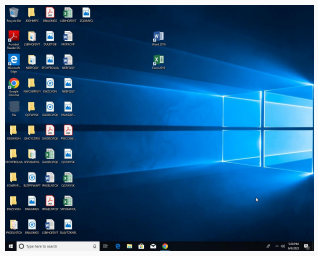
Windows Analysis Report

file.exe

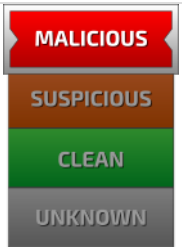
Overview

General Information

Sample Name:	file.exe
Analysis ID:	882707
MD5:	5e7d3490818e…
SHA1:	934454a655f32..
SHA256:	e498809a30ca…
Tags:	exe Glupteba
Infos:	



Detection



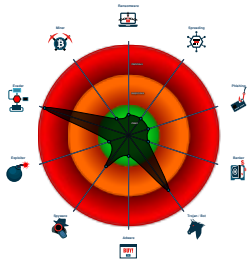
Glupteba

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Sigma detected: Schedule system p…
- Yara detected Glupteba
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Creates an autostart registry key po…
- Uses netsh to modify the Windows …
- Found Tor onion address
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 6760 cmdline: C:\Users\user\Desktop\file.exe MD5: 5E7D3490818E3F2A96F7A9DFC6950F9C)
  - powershell.exe (PID: 6824 cmdline: powershell -nologo -noprofile MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6816 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - file.exe (PID: 1488 cmdline: C:\Users\user\Desktop\file.exe MD5: 5E7D3490818E3F2A96F7A9DFC6950F9C)
      - powershell.exe (PID: 5576 cmdline: powershell -nologo -noprofile MD5: DBA3E6449E97D4E3DF64527EF7012A10)
        - conhost.exe (PID: 5984 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 2760 cmdline: C:\Windows\Sysnative\cmd.exe /C "netsh advfirewall firewall add rule name="csrss" dir=in action=allow program="C:\Windows\rss\csrss.exe" enable=yes" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 3432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - netsh.exe (PID: 6792 cmdline: netsh advfirewall firewall add rule name="csrss" dir=in action=allow program="C:\Windows\rss\csrss.exe" enable=yes MD5: 98CC37BBF363A38834253E22C80A8F32)
      - powershell.exe (PID: 7076 cmdline: powershell -nologo -noprofile MD5: DBA3E6449E97D4E3DF64527EF7012A10)
        - conhost.exe (PID: 6892 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 5848 cmdline: powershell -nologo -noprofile MD5: DBA3E6449E97D4E3DF64527EF7012A10)
        - conhost.exe (PID: 3372 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - csrss.exe (PID: 768 cmdline: C:\Windows\rss\csrss.exe MD5: 5E7D3490818E3F2A96F7A9DFC6950F9C)
        - powershell.exe (PID: 7012 cmdline: powershell -nologo -noprofile MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 6724 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - schtasks.exe (PID: 5760 cmdline: schtasks /CREATE /SC ONLOGON /RL HIGHEST /TR "C:\Windows\rss\csrss.exe" /TN csrss /F MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
          - conhost.exe (PID: 7136 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - schtasks.exe (PID: 6852 cmdline: schtasks /delete /tn ScheduledUpdate /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
          - conhost.exe (PID: 240 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - powershell.exe (PID: 2896 cmdline: powershell -nologo -noprofile MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 5124 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - powershell.exe (PID: 1360 cmdline: powershell -nologo -noprofile MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 5788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- TrustedInstaller.exe (PID: 6536 cmdline: C:\Windows\servicing\TrustedInstaller.exe MD5: 4578046C54A954C917BB393B70BA0AEB)
- csrss.exe (PID: 6772 cmdline: "C:\Windows\rss\csrss.exe" MD5: 5E7D3490818E3F2A96F7A9DFC6950F9C)
  - cmd.exe (PID: 2224 cmdline: C:\Windows\Sysnative\cmd.exe /C fodhelper MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 4768 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - fodhelper.exe (PID: 6780 cmdline: fodhelper MD5: 1D1F9E564472A9698F1BE3F9FEB9864B)
    - fodhelper.exe (PID: 4248 cmdline: "C:\Windows\system32\fodhelper.exe" MD5: 1D1F9E564472A9698F1BE3F9FEB9864B)
    - fodhelper.exe (PID: 6708 cmdline: "C:\Windows\system32\fodhelper.exe" MD5: 1D1F9E564472A9698F1BE3F9FEB9864B)

- csrss.exe (PID: 5596 cmdline: "C:\Windows\rss\csrss.exe" MD5: 5E7D3490818E3F2A96F7A9DFC6950F9C)
  - powershell.exe (PID: 1196 cmdline: powershell -nologo -noprofile MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6740 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - csrss.exe (PID: 6316 cmdline: C:\Windows\rss\csrss.exe MD5: 5E7D3490818E3F2A96F7A9DFC6950F9C)
    - powershell.exe (PID: 6652 cmdline: powershell -nologo -noprofile MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 6660 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- csrss.exe (PID: 2344 cmdline: C:\Windows\rss\csrss.exe MD5: 5E7D3490818E3F2A96F7A9DFC6950F9C)
  - powershell.exe (PID: 1364 cmdline: powershell -nologo -noprofile MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - csrss.exe (PID: 6216 cmdline: C:\Windows\rss\csrss.exe MD5: 5E7D3490818E3F2A96F7A9DFC6950F9C)
- csrss.exe (PID: 5280 cmdline: "C:\Windows\rss\csrss.exe" MD5: 5E7D3490818E3F2A96F7A9DFC6950F9C)
  - cmd.exe (PID: 6104 cmdline: C:\Windows\Sysnative\cmd.exe /C fodhelper MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 6140 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - fodhelper.exe (PID: 6048 cmdline: fodhelper MD5: 1D1F9E564472A9698F1BE3F9FEB9864B)
    - fodhelper.exe (PID: 5708 cmdline: "C:\Windows\system32\fodhelper.exe" MD5: 1D1F9E564472A9698F1BE3F9FEB9864B)
    - fodhelper.exe (PID: 6216 cmdline: "C:\Windows\system32\fodhelper.exe" MD5: 1D1F9E564472A9698F1BE3F9FEB9864B)
      - csrss.exe (PID: 6464 cmdline: "C:\Windows\rss\csrss.exe" MD5: 5E7D3490818E3F2A96F7A9DFC6950F9C)
        - powershell.exe (PID: 4680 cmdline: powershell -nologo -noprofile MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 4164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - csrss.exe (PID: 4472 cmdline: C:\Windows\rss\csrss.exe MD5: 5E7D3490818E3F2A96F7A9DFC6950F9C)
          - powershell.exe (PID: 2224 cmdline: powershell -nologo -noprofile MD5: DBA3E6449E97D4E3DF64527EF7012A10)
            - conhost.exe (PID: 6532 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 6184 cmdline: powershell -nologo -noprofile MD5: DBA3E6449E97D4E3DF64527EF7012A10)
        - conhost.exe (PID: 6200 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Glupteba	Glupteba is a trojan horse malware that is one of the top ten malware variants of 2021. After infecting a system, the Glupteba malware can be used to deliver additional malware, steal user authentication information, and enroll the infected system in a cryptomining botnet.	No Attribution	**http://** resources.infosecinstitute.com/tdss4-part-1/https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-malware/https://blog.google/technology/safety-security/new-action-combat-cyber-crime/https://blog.google/threat-analysis-group/disrupting-glupteba-operation/https://blog.sekoia.io/privateloader-the-loader-of-the-prevalent-ruzki-ppi-service/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.glupteba

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.400548532.0000000000843000.00000040.00000001.01000000.00000003.sdmp	JoeSecurity_Glupteba	Yara detected Glupteba	Joe Security	
0000003C.00000002.570772687.0000000003843000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Glupteba	Yara detected Glupteba	Joe Security	
00000005.00000002.403769101.0000000002BA3000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x798:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000029.00000002.480076167.0000000000843000.00000040.00000001.01000000.00000005.sdmp	JoeSecurity_Glupteba	Yara detected Glupteba	Joe Security	
0000001C.00000002.599256866.0000000003843000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Glupteba	Yara detected Glupteba	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 61 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
22.2.csrss.exe.3a22567.14.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth (Nextron Systems)	• 0x39858:$s2: The Magic Word! • 0x45998:$s2: The Magic Word! • 0x39bb8:$s3: Software\Oracle\VirtualBox • 0x39847:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73
64.2.csrss.exe.a32420.4.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth (Nextron Systems)	• 0x29b38:$s2: The Magic Word! • 0x35c78:$s2: The Magic Word! • 0x29e98:$s3: Software\Oracle\VirtualBox • 0x29b27:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73
28.2.csrss.exe.a1cb00.3.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth (Nextron Systems)	• 0x3f458:$s2: The Magic Word! • 0x4b598:$s2: The Magic Word! • 0x3f7b8:$s3: Software\Oracle\VirtualBox • 0x3f447:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73
60.2.csrss.exe.3a1c967.14.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth (Nextron Systems)	• 0x3f458:$s2: The Magic Word! • 0x4b598:$s2: The Magic Word! • 0x3f7b8:$s3: Software\Oracle\VirtualBox • 0x3f447:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73
28.2.csrss.exe.3a32287.13.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth (Nextron Systems)	• 0x29b38:$s2: The Magic Word! • 0x35c78:$s2: The Magic Word! • 0x29e98:$s3: Software\Oracle\VirtualBox • 0x29b27:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73
Click to see the 118 entries				

Sigma Signatures

Persistence and Installation Behavior

Sigma detected: Schedule system process

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected Glupteba

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Bitcoin Miner

Yara detected Glupteba

Compliance

Detected unpacking (overwrites its own PE header)

Networking

Found Tor onion address

Performs DNS queries to domains with low reputation

E-Banking Fraud

Yara detected Glupteba

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Persistence and Installation Behavior

Creates files in the system32 config directory

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

Drops PE files with benign system names

Boot Survival

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

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

Malware Analysis System Evasion

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

HIPS / PFW / Operating System Protection Evasion

Performs DNS TXT record lookups

Lowering of HIPS / PFW / Operating System Security Settings

Uses netsh to modify the Windows network and firewall settings

Modifies the windows firewall

Stealing of Sensitive Information

Yara detected Glupteba

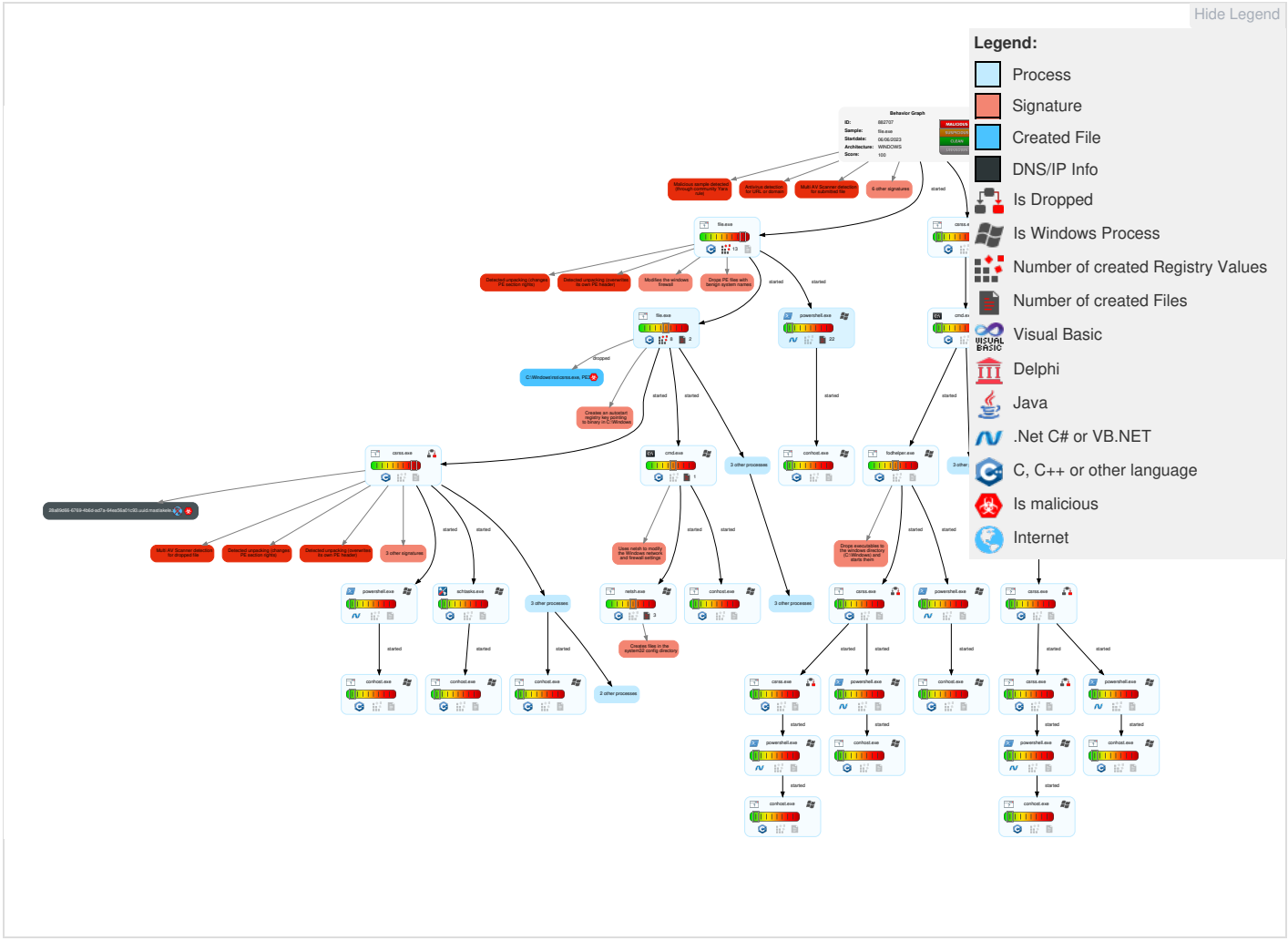
Remote Access Functionality

Yara detected Glupteba

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	2 1 Windows Management Instrumentation	1 Windows Service	1 Windows Service	3 2 1 Masquerading	1 Input Capture	2 3 1 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Non-Application Layer Protocol	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Command and Scripting Interpreter	1 Scheduled Task/Job	1 1 Process Injection	2 Disable or Modify Tools	LSASS Memory	4 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	1 1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	4 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Proxy	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 1 Registry Run Keys / Startup Folder	1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 File and Directory 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	2 Software Packing	Cached Domain Credentials	1 3 System Information Discovery	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 File Deletion	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

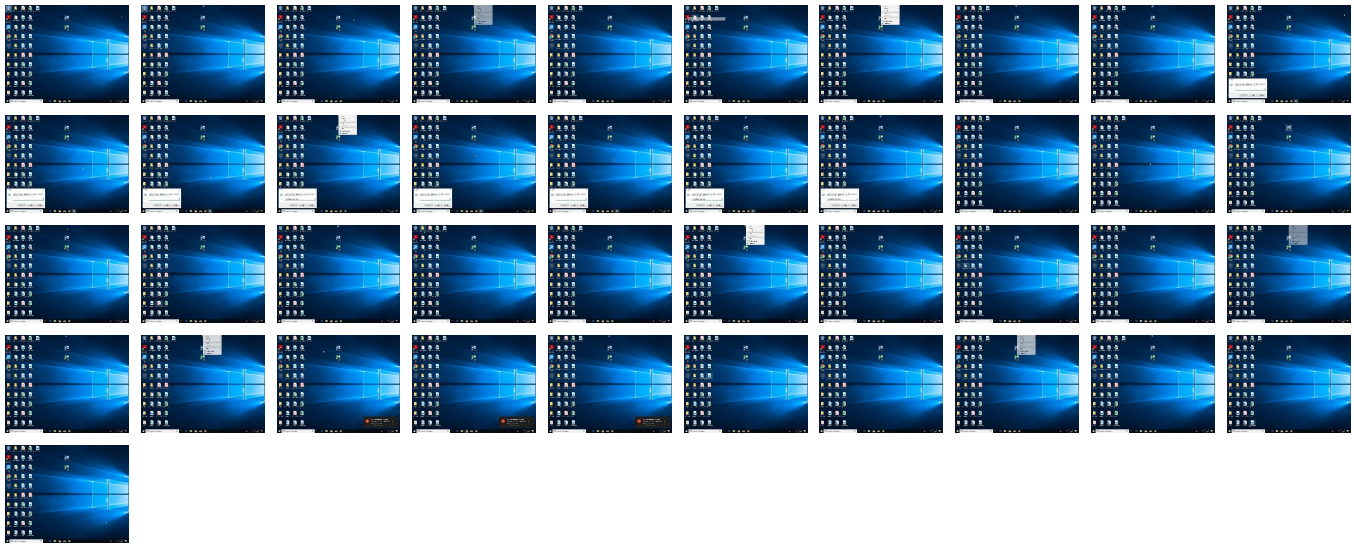
Behavior Graph



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
file.exe	76%	ReversingLabs	Win32.Trojan.RedLine	
file.exe	80%	Virustotal		Browse
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\rss\csrss.exe	100%	Joe Sandbox ML		
C:\Windows\rss\csrss.exe	76%	ReversingLabs	Win32.Trojan.RedLine	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.alltheweb.com/help/webmaster/crawler)Mozilla/5.0	0%	URL Reputation	safe	
http://invalidlog.txtlookup	0%	URL Reputation	safe	
http://gais.cs.ccu.edu.tw/robot.php)Gulper	0%	URL Reputation	safe	
http://devlog.gregarius.net/docs/ua)Links	0%	URL Reputation	safe	
http://www.google.	0%	URL Reputation	safe	
http://misc.yahoo.com.cn/help.html)QueryPerformanceFrequency	0%	URL Reputation	safe	
http://www.spidersoft.com)Wg	0%	Avira URL Cloud	safe	
http://vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.oniontls:	0%	Avira URL Cloud	safe	
http://un6fsy7wsdbqb54aridsmu5mtdcctatumigg37ip476tsdy2jf6ascqd.onionC:	0%	Avira URL Cloud	safe	
http://crl.g	0%	URL Reputation	safe	
http://https://blockchain.infoindex	0%	URL Reputation	safe	
http://https://mastiakele.xyzun6fsy7wsdbqb54aridsmu5mtdcctatumigg37ip476tsdy2jf6ascqd.onionhttps://m	0%	Avira URL Cloud	safe	
http://www.exabot.com/go/robot)Opera/9.80	0%	URL Reputation	safe	
http://www.googlebot.com/bot.html)Links	0%	URL Reputation	safe	
http://https://mastiakele.xyzhttps://mastiakele.xyzRegQueryValueExWhttps://mastiakele.xyzUUIDUUIDPGDSEPGDSE	0%	Avira URL Cloud	safe	
http://https://_bad_pdb_file.pdb	0%	Avira URL Cloud	safe	
http://un6fsy7wsdbqb54aridsmu5mtdcctatumigg37ip476tsdy2jf6ascqd.onionS-1-5-21-3853321935-2125563209-	0%	Avira URL Cloud	safe	
http://https://raw.githubusercontent.com/spesmilo/electrum/master/electrum/servers.jsonsize	0%	Avira URL Cloud	safe	
http://grub.org)Mozilla/5.0	0%	Avira URL Cloud	safe	
http://www.avantbrowser.com)MOT-V9mm/00.62	0%	Avira URL Cloud	safe	
http://localhost:3433/https://duniadekho.baridna:	0%	Avira URL Cloud	safe	
http://https://mastiakele.xyzun6fsy7wsdbqb54aridsmu5mtdcctatumigg37ip476tsdy2jf6ascqd.onionCommonPro	0%	Avira URL Cloud	safe	
http://www.bloglines.com)Frame	0%	Avira URL Cloud	safe	
http://https://mastiakele.xyzhttps://mastiakele.xyzRegQueryValueExWUUIDPGDSE64-bitc:	0%	Avira URL Cloud	safe	
http://https://mastiakele.xyzun6fsy7wsdbqb54aridsmu5mtdcctatumigg37ip476tsdy2jf6ascqd.onion	0%	Avira URL Cloud	safe	
http://un6fsy7wsdbqb54aridsmu5mtdcctatumigg37ip476tsdy2jf6ascqd.onionhttp://un6fsy7wsdbqb54aridsmu5m	0%	Avira URL Cloud	safe	
http://https://mastiakele.xyzMicrosoft	0%	Avira URL Cloud	safe	
http://un6fsy7wsdbqb54aridsmu5mtdcctatumigg37ip476tsdy2jf6ascqd.onion	100%	Avira URL Cloud	malware	
http://https://mastiakele.xyz	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
28a89d66-6769-4b6d-ad7a-64ea56a01c93.uuid.mastiakele.xyz	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.spidersoft.com)Wg	file.exe	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.msn.com/msnbot.htm)net/http:	file.exe, 00000000.00000003.342311330.00000000003760000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000000.00000002.360923805.0000000000400000.00000040.00000001.01000000.00000003.sdmp, file.exe, 00000000.00000002.364753333.0000000002E70000.00000040.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.400548532.0000000000400000.00000040.00000001.01000000.00000003.sdmp, file.exe, 00000005.00000003.362103364.0000000003890000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.414419556.0000000002FA0000.00000040.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.624848873.0000000003400000.00000040.00001000.00020000.00000000.sdmp	false		high
http://www.alltheweb.com/help/webmaster/crawler)Mozilla/5.0	file.exe	false	• URL Reputation: safe	unknown
http://yandex.com/	file.exe	false		high
http://search.msn.com/msnbot.htm)net/htt	file.exe	false		high
http://un6fsy7wsdbqb54aridsmu5mtdcctatumigg37ip476tsdy2jf6ascqd.onionC:	file.exe, 00000005.00000002.424748729.0000000C01A000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.google.com/bot.html)crypto/ecdh:	file.exe	false		high
http://vcr4vuv4sf5233btfy7xboezl7umjw7rljdmaeztmmf4s6k2ivinj3yd.oniontls:	file.exe	true	• Avira URL Cloud: safe	unknown
http://https://github.com/Snawoot/opera-proxy/releases/download/v1.2.2/opera-p	file.exe	false		high
http://invalidlog.txtlookup	file.exe, file.exe, 00000005.00000002.400548532.0000000000400000.00000040.00000001.01000000.00000003.sdmp, file.exe, 00000005.00000003.362103364.0000000003890000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.414419556.0000000002FA0000.00000040.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.624848873.0000000003400000.00000040.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://search.msn.com/msnbot.htm)msnbot/1.1	file.exe, file.exe, 00000005.00000002.400548532.0000000000400000.00000040.00000001.01000000.00000003.sdmp, file.exe, 00000005.00000003.362103364.0000000003890000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.414419556.0000000002FA0000.00000040.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.624848873.0000000003400000.00000040.00001000.00020000.00000000.sdmp	false		high
http://gais.cs.ccu.edu.tw/robot.php)Gulper	file.exe	false	• URL Reputation: safe	unknown
http://https://mastiakele.xyzun6fsy7wsdbqb54aridsmu5mtdcctatumigg37ip476tsdy2jf6ascqd.onionhttps://m	file.exe, 00000000.00000002.378648564.0000000C0A2000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.archive.org/details/archive.org_bot)Opera/9.80	file.exe	false		high
http://www.baidu.com/search/spider.htm)MobileSafari/600.1.4	file.exe, file.exe, 00000005.00000002.400548532.0000000000400000.00000040.00000001.01000000.00000003.sdmp, file.exe, 00000005.00000003.362103364.0000000003890000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.414419556.0000000002FA0000.00000040.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.624848873.0000000003400000.00000040.00001000.00020000.00000000.sdmp	false		high
http://yandex.com/bots)Opera/9.51	file.exe	false		high
http://www.google.com/bot.html)Mozilla/5.0	file.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://mastiakele.xyz	file.exe, 00000000.00000002.378648564.00000000C090000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000000.00000002.378648564.000000000C0A2000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.424748729.000000000C016000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.424748729.000000000C00E000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.627457527.000000000C80E000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.627457527.000000000C816000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://mastiakele.xyzhttps://mastiakele.xyzRegQueryValueExWhttps://mastiakele.xyzUUIDUUIDPGDSEPGDSE	file.exe, 00000000.00000002.378648564.00000000C090000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://_bad_pdb_file.pdb	file.exe, 00000000.00000003.342311330.00000003E2B000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000000.00000002.364753333.000000000353B000.00000040.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.400548532.00000000ACC000.00000040.00000001.01000000.00000003.sdmp, file.exe, 00000005.00000002.414419556.000000000366B000.00000040.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.624848873.0000000003ACB000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://archive.org/details/archive.org_bot)Mozilla/5.0	file.exe	false		high
http://devlog.gregarius.net/docs/ua)Links	file.exe, file.exe, 00000005.00000002.400548532.00000000400000.00000040.00000001.01000000.00000003.sdmp, file.exe, 00000005.00000003.362103364.0000000003890000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.414419556.00000000002FA0000.00000040.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.624848873.0000000003400000.00000040.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.google.	file.exe	false	• URL Reputation: safe	unknown
http://misc.yahoo.com.cn/help.html)QueryPerformanceFrequency	file.exe	false	• URL Reputation: safe	unknown
http://help.yahoo.com/help/us/ysearch/slurp)SonyEricssonK550i/R1JD	file.exe	false		high
http://www.avantbrowser.com	file.exe	false		high
http://un6fsy7wsdbqb54aridsmu5mtdcctatumigg37ip476tsdy2jf6ascqd.onionS-1-5-21-3853321935-2125563209-	file.exe, 00000005.00000002.424748729.000000000C00E000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.627457527.000000000C80E000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	low
http://https://mastiakele.xyzMicrosoft	file.exe, 00000005.00000002.424748729.000000000C00E000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.424748729.000000000C072000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.627457527.000000000C858000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.627457527.000000000C80E000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.google.com/feedfetcher.html)HKLM	file.exe, file.exe, 00000005.00000002.400548532.00000000400000.00000040.00000001.01000000.00000003.sdmp, file.exe, 00000005.00000003.362103364.0000000003890000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.414419556.00000000002FA0000.00000040.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.624848873.0000000003400000.00000040.00001000.00020000.00000000.sdmp	false		high
http://grub.org)Mozilla/5.0	file.exe	false	• Avira URL Cloud: safe	low
http://https://cdn.discordapp.com/attachments/1087398815188910163/1087399133926674453/LZ.zipreflect.Value.I	file.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://raw.githubusercontent.com/spesmilo/electrum/master/electrum/servers.jsonsize	file.exe	false	• Avira URL Cloud: safe	unknown
http://crl.g	file.exe, 00000000.00000002.363521570.0000000002A72000.00000040.00000020.00020000.00000000.sdmp, file.exe, 00000005.00000002.403769101.0000000002BA3000.00000040.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://blockchain.infoindex	csrss.exe, 0000000F.00000002.624848873.000000003400000.00000040.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.avantbrowser.com)MOT-V9mm/00.62	file.exe, 00000000.00000003.342311330.00000003760000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000000.00000002.360923805.0000000000400000.00000040.00000001.01000000.00000003.sdmp, file.exe, 00000000.00000002.364753333.0000000002E70000.00000040.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.400548532.0000000000400000.00000040.00000001.01000000.00000003.sdmp, file.exe, 00000005.00000003.362103364.0000000003890000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.414419556.000000002FA0000.00000040.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.624848873.0000000003400000.00000040.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://turnitin.com/robot/crawlerinfo.html)cannot	file.exe, file.exe, 00000005.00000002.400548532.0000000000400000.00000040.00000001.01000000.00000003.sdmp, file.exe, 00000005.00000003.362103364.0000000003890000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.414419556.000000002FA0000.00000040.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.624848873.0000000003400000.00000040.00001000.00020000.00000000.sdmp	false		high
http://localhost:3433/https://duniadekho.baridna:	file.exe, file.exe, 00000005.00000002.400548532.0000000000400000.00000040.00000001.01000000.00000003.sdmp, file.exe, 00000005.00000003.362103364.0000000003890000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.414419556.000000002FA0000.00000040.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.624848873.0000000003400000.00000040.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	low
http://un6fsy7wsdbqb54aridsmu5mtdcctatumigg37ip476tsdy2jf6ascqd.onion	file.exe, 00000000.00000002.378648564.0000000C0DE000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000000.00000002.378648564.000000000C0A2000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.424748729.0000000000C00E000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.627457527.000000000C80E000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.exabot.com/go/robot)Opera/9.80	file.exe	false	• URL Reputation: safe	unknown
http://search.msn.com/msnbot.htm)pkcs7:	file.exe, file.exe, 00000005.00000002.400548532.0000000000400000.00000040.00000001.01000000.00000003.sdmp, file.exe, 00000005.00000003.362103364.0000000003890000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.414419556.000000002FA0000.00000040.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.624848873.0000000003400000.00000040.00001000.00020000.00000000.sdmp	false		high
http://https://mastiakele.xyzun6fsy7wsdbqb54aridsmu5mtdcctatumigg37ip476tsdy2jf6ascqd.onionCommonPro	file.exe, 00000000.00000002.378648564.0000000C092000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.426549971.000000000C11E000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.629197861.000000000C91E000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.alexa.com/help/webmasters;	file.exe	false		high
http://www.google.com/adsbot.html)Encountered	file.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://mastiakele.xyzhttps://mastiakele.xyzRegQueryValueExWUUIDPGDSE64-bitc:	file.exe, 00000005.00000002.424748729.000000000C016000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.627457527.000000000C816000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bloglines.com)Frame	file.exe	false	• Avira URL Cloud: safe	low
http://https://mastiakele.xyzun6fsy7wsdbqb54aridsmu5mtdcctatumigg37ip476tsdy2jf6ascqd.onion	file.exe, 00000000.00000002.378648564.000000000C0E6000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.624321444.000000000105A000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://un6fsy7wsdbqb54aridsmu5mtdcctatumigg37ip476tsdy2jf6ascqd.onionhttp://un6fsy7wsdbqb54aridsmu5m	file.exe, 00000000.00000002.378648564.000000000C0DE000.00000004.00001000.00020000.00000000.sdmp, file.exe, 00000005.00000002.424748729.000000000C00E000.00000004.00001000.00020000.00000000.sdmp, csrss.exe, 0000000F.00000002.627457527.000000000C80E000.00000004.00001000.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.googlebot.com/bot.html)Links	file.exe	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882707
Start date and time:	2023-06-06 17:17:17 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	66
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	file.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@79/32@1/0
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 27.5% (good quality ratio 13.2%) • Quality average: 40.1% • Quality standard deviation: 44.2%
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, consent.exe, WMIADAP.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Execution Graph export aborted for target file.exe, PID 6760 because there are no executed function
- 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 NtOpenKeyEx calls found.

- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:18:18	API Interceptor	7x Sleep call for process: file.exe modified
17:18:23	API Interceptor	330x Sleep call for process: powershell.exe modified
17:18:46	API Interceptor	9x Sleep call for process: csrss.exe modified
17:18:46	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run csrss "C:\Windows\rss\csrss.exe"
17:18:56	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run csrss "C:\Windows\rss\csrss.exe"
17:18:57	Task Scheduler	Run new task: csrss path: C:\Windows\rss\csrss.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\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Reputation:	unknown

Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

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

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22204
Entropy (8bit):	5.459012652297042
Encrypted:	false
SSDEEP:	384:7tCRL0YyLr2AfLNSVud7WjbPsJa1QQ1C5SeO8vH4b60mwXJpiprg:iyn3fBUud7a/QjTP4uvCp5
MD5:	AD1C21EEB0DAC1C77F3EF5AD7FA46A7D
SHA1:	17E154771EF4DEE59BB98668F671BAB2CCCFDB93
SHA-256:	AD83FC496FDB8A1F66C7359293721288833C649BD2AEAE104EC307CB256B5BD6
SHA-512:	E6F3D9005ACBD7D64A200D63A37DEE562B1C2CDC8E5CAA5A171E78DC4001804905A81CC12A9CDEFC052D1E8618C1B54A358C1CE4BAB793B789B83333DBAB BF0A
Malicious:	false
Reputation:	unknown
Preview:	@...e.....e.....@.....H.....<@.^.L."My...:I.... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automati on4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microso ft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....Syste m.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Trans actions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....Sy stem.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0hiwndk4.bpq.psm1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1kmi0cxx.czu.psm1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_neh5uxb5.2du.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_r24lykxa.jtx.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_s4hshgl2.ban.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xxox1cid.pwx.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U

MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yfxhgdjq.5aw.ps1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yz2x05go.ann.psm1

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

C:\Windows\Logs\CBS\CBS.log

Process:	C:\Windows\servicing\TrustedInstaller.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (315), with CRLF line terminators
Category:	modified
Size (bytes):	3080192
Entropy (8bit):	5.307629755331727
Encrypted:	false
SSDEEP:	6144:TLS5YygL1mnGVFQa/qJIxOfTFyKQel5lmhSVjfChq4TMmdqj3:TL1dq
MD5:	84284E25CC68C93D0D4AC6319713FA6C
SHA1:	C79240F519C0CE886F20A0B603C7741639F329FA
SHA-256:	72ED1E9104F4941C2A30EF3951F42E8BE5DB2789FC28D6108E89EFC2AE8654CE
SHA-512:	EEFDA1D5C2A0390F9D096B75DA4B5B3C62E6DA2BDED9A33D0CB7D707C1A62E2EC162B1D105F3F7426EE167DF02904E11462992CD249C16460D5B0AEC28A14 74
Malicious:	false
Reputation:	unknown

Preview:	.2019-06-27 00:55:29, Info CBS TI: --- Initializing Trusted Installer ---..2019-06-27 00:55:29, Info CBS TI: Last boot time: 2019-06-27 00:49:51.660..2019-06-27 00:55:29, Info CBS Starting TrustedInstaller initialization...2019-06-27 00:55:29, Info CBS Lock: New lock added: CCbsPublicSessionClassFactory, level: 30, total lock:4..2019-06-27 00:55:29, Info CBS Lock: New lock added: CCbsPublicSessionClassFactory, level: 30, total lock:5..2019-06-27 00:55:29, Info CBS Lock: New lock added: WinlogonNotifyLock, level: 8, total lock:6..2019-06-27 00:55:29, Info CBS Ending TrustedInstaller initialization...2019-06-27 00:55:29, Info CBS Starting the TrustedInstaller main loop...2019-06-27 00:55:29, Info CBS TrustedInstaller service starts successfully...2019-06-27 00:55:29, Info CBS No startup pr

C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22092
Entropy (8bit):	5.599604238208506
Encrypted:	false
SSDEEP:	384:xtCRo089Iocj0aKiLSBTKpUyucFzFjjP971ea5cO9fgSe1yvB4Iz60lTXLpiOUx:coovL4+5uOlR71TFOGZ4Jwpe
MD5:	BFA918656378264D5004CC1470E162BB
SHA1:	787B0B440203F5DB0025F15F8D5AB740759ECB80
SHA-256:	43A9F755F97F0CD8DC8661AB6D120735F8B61C5244D6299667E57D50DB53BDC7
SHA-512:	31CAB5D79FA45A4403AE0CF4EF08CD15FBC0CF94FDC110423C958E7F64B05270F48DD695538F246F04F9BD3C7AAA6DCDE03972422544704BA9887D5DEDBA3B66
Malicious:	false
Reputation:	unknown
Preview:	@...e.....J.....a.O.O.....+.....@.....H.....<@.^.L."My...:I..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Windows\Temp__PSScriptPolicyTest_1ufz0sgk.myo.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Windows\Temp__PSScriptPolicyTest_4kbnorl3.12h.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Windows\Temp__PSScriptPolicyTest_5rosccoi.3tj.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Windows\Temp__PSScriptPolicyTest_5z2r5jwu.tvo.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Windows\Temp__PSScriptPolicyTest_alrlhr1g.v5f.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Windows\Temp__PSScriptPolicyTest_llc3eusd.wzr.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U

MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Windows\Temp__PSScriptPolicyTest_m40tnpqs.odn.psm1

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

C:\Windows\Temp__PSScriptPolicyTest_mcrmpiy0.i5p.psm1

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

C:\Windows\Temp__PSScriptPolicyTest_ninjjd0h.sdc.psm1

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

C:\Windows\Temp__PSScriptPolicyTest_p2nuu3nn.1zm.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Windows\Temp__PSScriptPolicyTest_phccmwlw.m0k.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Windows\Temp__PSScriptPolicyTest_q5tugduk.fnu.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Windows\Temp__PSScriptPolicyTest_tegyafc1.bwe.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false

SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Windows\Temp__PSScriptPolicyTest_txvnygx2.3pj.ps1

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

C:\Windows\Temp__PSScriptPolicyTest_vvhtfm1i.slt.psm1

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

C:\Windows\Temp__PSScriptPolicyTest_w0aevyid.a34.psm1

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

C:\Windows\Temp__PSScriptPolicyTest_yjogpmn2.2vt.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Windows\Temp__PSScriptPolicyTest_z5j1xn30.oha.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Windows\rss\csrss.exe	
Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4377472
Entropy (8bit):	7.9744939964113035
Encrypted:	false
SSDEEP:	98304:6tF4ah6fnbBWKRFjbBoWQaZBcADzh9LZIm9riDYPhtZj:1c6foKbBzDcADzhht5F
MD5:	5E7D3490818E3F2A96F7A9DFC6950F9C
SHA1:	934454A655F32B4645CE827B3A39BED2CF5D891C
SHA-256:	E498809A30CAB90E8D5EB3FF4610BC177EA9E63110530DA50643332263F4AB55
SHA-512:	6E94AFCC7027D56A9AD19CC687766A4DAB407314B622128200EBC84EBFB6A5F9F8A29F9DA7A6CE5DB0EC7A96CB9992FC964430818426468A59D222D054E3C2 A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 76%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:].[3..[3..[3.....[3.....[3.....[3...H..[3..[2.;[3.....[3.....[3.....[3.Rich. [3.....PE..L.....c.....@..L&.....)H.....@...@.....I.C.....x.@.d.... e.....B.....P..... .....X0..@..... .....text...&.@.....@..... ..`.data...HX$...@.....@.....@....rsrc...',.. e.....@.....@..@.reloc...Z...P...Z...fB.....@..B..... ....

\Device\Null	
Process:	C:\Windows\rss\csrss.exe

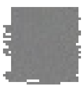
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	2005
Entropy (8bit):	5.199889815210355
Encrypted:	false
SSDEEP:	24:EEDi2++lqD+0qt0vi1x8/ko+3bd+e2Td0dxWs9xD+FuN1c8t0vndauS/ko+3bdhb:0+QTqtpxM+YO/9x6CG8ticL+3OtZL+37
MD5:	85F8EE5B629AA6A997426FCA1F18AE12
SHA1:	CD0D07D4F353E1F4797C07E36DBE77C2B3487A4C
SHA-256:	06052F50A0750BF5F1EA92A2EFA2ADD285CE8E78562A3866A80EDC85D3C8EB4F
SHA-512:	24339EF07C1C66AC7F17CF484E694516450B2DF7A4C0D2187989185FFF5059A942847ED698C1E12384CCD383958AEE87A40671899B1108D455AE47A54A183CC9
Malicious:	false
Reputation:	unknown
Preview:	2023/06/06 17:18:46 current filenname with args "C:\Windows\rss\csrss.exe".2023/06/06 17:18:56 disable cloud protection: exit status 1: PS C:\Windows\rss> Set-MpPreference -MAPSReporting Disabled.Set-MpPreference : Operation failed with the following error: 0x800106ba. Operation: Set-MpPreference. Target: ..MAPS_MAPSReporting...At line:1 char:1..+ Set-MpPreference -MAPSReporting Disabled..+ ~~~~~~.. + CategoryInfo : NotSpecified: (MSFT_MpPreference:root\Microsoft\...FT_MpPreference) [Set-MpPreference], .. CimException.. + FullyQualifiedErrorId : HRESULT 0x800106ba,Set-MpPreference.. ..PS C:\Windows\rss> .2023/06/06 17:18:56 initial server https://server3.mastiakele.xyz.2023/06/06 17:18:56 first install, ignore discover on start. 2023/06/06 17:19:02 add defender path exclusions: exit status 1: PS C:\Windows\rss> Add-MpPreference -ExclusionPath "C:\Windows\rss", "C:\Users\user\AppData\Local\Temp\csrss", "C:\Windows\windefender.exe",

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.9744939964113035
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:	file.exe
File size:	4377472
MD5:	5e7d3490818e3f2a96f7a9dfc6950f9c
SHA1:	934454a655f32b4645ce827b3a39bed2cf5d891c
SHA256:	e498809a30cab90e8d5eb3ff4610bc177ea9e63110530da50643332263f4ab55
SHA512:	6e94afcc7027d56a9ad19cc687766a4dab407314b622128200ebc84ebfb6a5f9f8a29f9da7a6ce5db0ec7a96cb9992fc964430818426468a59d222d054e3c24a
SSDEEP:	98304:6tF4ah6fnbBWKRFjbBoWQaZBcADzh9LZIm9riDYPhtZj:1c6foKbBzDcADzhht5F
TLSH:	E4162353D295BD50D9AB4A73AF2FC6F87A1DF4108F563B6A02298E1F1472772D1A3B00
File Content Preview:	MZ....................@...!..L.!This program cannot be run in DOS mode....$........:]..[3..[3..[3......[3......[3......[3...H..[3..[2.;[3......[3......[3......[3.Rich.[3.........PE..L......c.................@

File Icon



Icon Hash:	454545556145691d

Static PE Info

General

Entrypoint:	0x404829
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x6385D2BC [Tue Nov 29 09:37:00 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0

File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	96475f7ea3cc105ae1bb971e987af868

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN=522b1f00070a2734475a3201002b1c42301c1b0732151b1d231030330b0713013107, PostalCode=10802, S=0b1c1115005f5c4e1802161701040e1609164f0d1a1f + S=0b1c1115494a5c141b5503101152120001111017565102 1a0c0100080654181701000b110407101e0812045654011551445307121 11a57090e53040 602055b0c0b0a070b
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 5/28/2023 10:15:45 AM 5/27/2024 10:15:45 AM
Subject Chain	• CN=522b1f00070a2734475a3201002b1c42301c1b0732151b1d231030330b0713013107, PostalCode=10802, S=0b1c1115005f5c4e1802161701040e1609164f0d1a1f + S=0b1c1115494a5c141b5503101152120001111017565102 1a0c0100080654181701000b110407101e0812045654011551445307121 11a57090e53 000602055b0c0b0a070b
Version:	3
Thumbprint MD5:	FA53284E976FB57C511F84800D1026E7
Thumbprint SHA-1:	AAB41FBA0BFBA63477C31EE1F81BACD1C7823717
Thumbprint SHA-256:	53CC9B394A0EAA065DA50259374B3E3F028D96EC454727111A05CB9D11C9958F
Serial:	5A3B83BA33D148511EE69564FACB49F1

Entrypoint Preview
Instruction
call 00007FD1509E1603h
jmp 00007FD1509DCF9Dh
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007FD1509DD146h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007FD1509DD170h
test ecx, 00000003h
jne 00007FD1509DD111h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007FD1509DD10Ah

Instruction
mov eax, dword ptr [ecx-04h]
test al, al
je 00007FD1509DD154h
test ah, ah
je 00007FD1509DD146h
test eax, 00FF0000h
je 00007FD1509DD135h
test eax, FF000000h
je 00007FD1509DD124h
jmp 00007FD1509DD0EFh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 20h
mov eax, dword ptr [ebp+08h]
push esi
push edi
push 00000008h
pop ecx
mov esi, 004012D8h
lea edi, dword ptr [ebp-20h]
rep movsd
mov dword ptr [ebp-08h], eax
mov eax, dword ptr [ebp+0Ch]
pop edi
mov dword ptr [ebp-04h], eax
pop esi

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [C++] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x40af78	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x652000	0x197f8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x42c000	0xb80	.data
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x915000	0xdc8	.reloc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1220	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x3058	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1cc	.text
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	0x40aa26	0x40ac00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x40c000	0x245848	0x1e00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x652000	0x2c27f8	0x19800	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x915000	0x5a00	0x5a00	False	0.13307291666666668	data	1.581416306261645	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x652730	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x6535d8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x653e80	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x656428	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x6574d0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x657988	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x658830	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x6590d8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x659640	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x65bbe8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x65cc90	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x65d618	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x65dae8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x65e990	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x65f238	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0		
RT_ICON	0x65f900	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x65fe68	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x662410	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x6634b8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x663988	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x664830	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x6650d8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x665640	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x667be8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x668c90	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x669618	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_STRING	0x669d20	0x5c4	data		
RT_STRING	0x66a2e8	0x710	data		
RT_STRING	0x66a9f8	0x558	data		
RT_STRING	0x66af50	0x29c	data		
RT_STRING	0x66b1f0	0x606	data		
RT_GROUP_ICON	0x669a80	0x68	data		
RT_GROUP_ICON	0x657938	0x4c	data		
RT_GROUP_ICON	0x663920	0x68	data		
RT_GROUP_ICON	0x65da80	0x68	data		
RT_VERSION	0x669ae8	0x238	data		

Imports

DLL	Import
KERNEL32.dll	VirtualFree, IsBadReadPtr, GetConsoleAliasesLengthA, WaitForMultipleObjectsEx, FreeConsole, GetVersionExW, WritePrivateProfileStructW, IsProcessorFeaturePresent, MulDiv, EnumResourceLanguagesA, GetModuleFileNameW, CreateActCtxA, WritePrivateProfileStringW, ReplaceFileA, GetStringTypeExA, GetStdHandle, GetLogicalDriveStringsA, OpenMutexW, GetLastError, ReadConsoleOutputCharacterA, GetModuleHandleW, AttachConsole, VirtualAlloc, LoadLibraryA, InterlockedExchangeAdd, LocalAlloc, GetFileType, CreateFileMappingW, FindFirstVolumeMountPointW, GetNumberFormatW, CreateEventW, GetModuleFileNameA, lstrcmpiW, GetModuleHandleA, CreateMutexA, CancelTimerQueueTimer, GetFileAttributesExW, GetConsoleCursorInfo, ScrollConsoleScreenBufferA, GetCurrentThreadId, FindAtomW, DebugBreak, FindNextVolumeA, AddConsoleAliasW, CancelWaitableTimer, GetCommState, WaitForSingleObject, GetProcAddress, GetCommandLineA, GetStartupInfoA, RaiseException, RtlUnwind, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapAlloc, HeapFree, EnterCriticalSection, LeaveCriticalSection, SetHandleCount, DeleteCriticalSection, Sleep, ExitProcess, WriteFile, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, InterlockedDecrement, HeapCreate, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, HeapReAlloc, SetFilePointer, GetConsoleCP, GetConsoleMode, InitializeCriticalSectionAndSpinCount, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, HeapSize, FlushFileBuffers, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, CloseHandle, CreateFileA
USER32.dll	CharLowerBuffA
GDI32.dll	EnumFontsW, GetCharABCWidthsFloatA, GetCharWidthW
ADVAPI32.dll	MapGenericMask

Network Behavior

UDP Packets

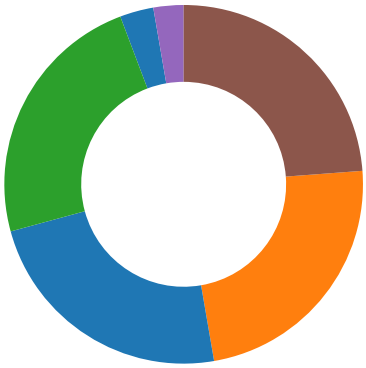
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 6, 2023 17:18:55.956470013 CEST	61178	53	192.168.2.7	8.8.8.8
Jun 6, 2023 17:18:56.020364046 CEST	53	61178	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 6, 2023 17:18:55.956470013 CEST	192.168.2.7	8.8.8.8	0x11d	Standard query (0)	28a89d66-6769-4b6d-ad7a-64ea56a01c93.uuid.mastiakele.xyz	16	IN (0x0001)	false

Statistics

Behavior



- file.exe
- powershell.exe
- conhost.exe
- TrustedInstaller.exe
- file.exe
- powershell.exe
- conhost.exe
- cmd.exe
- conhost.exe
- netsh.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- csrss.exe
- powershell.exe
- conhost.exe
- schtasks.exe
- csrss.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- powershell.exe
- conhost.exe
- csrss.exe
- cmd.exe
- conhost.exe
- fodhelper.exe
- fodhelper.exe
- fodhelper.exe
- powershell.exe
- conhost.exe
- csrss.exe
- csrss.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- cmd.exe
- conhost.exe
- fodhelper.exe
- fodhelper.exe
- fodhelper.exe
- csrss.exe
- csrss.exe
- powershell.exe
- conhost.exe
- powershell.exe
- conhost.exe
- csrss.exe
- powershell.exe
- conhost.exe
- csrss.exe
- powershell.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: file.exe PID: 6760, Parent PID: 3320

General

Target ID:	0
Start time:	17:18:16

Start date:	06/06/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	4377472 bytes
MD5 hash:	5E7D3490818E3F2A96F7A9DFC6950F9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000000.00000003.342311330.0000000003760000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000000.00000003.342311330.0000000003BA1000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000000.00000002.364753333.00000000032B3000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.363521570.0000000002A72000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000000.00000002.360923805.0000000000843000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000000.00000002.360923805.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.364753333.0000000002E70000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Registry Activities

Analysis Process: powershell.exe PID: **6824**, Parent PID: **6760**

General

Target ID:	1
Start time:	17:18:19
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xe60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71D65B28	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	71D65B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_s4hshgl2.ban.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71E01E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0hiwndk4.bpq.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71E01E60	CreateFileW
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	72EBCF06	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	72EBCF06	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	73081926	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_s4hshgl2.ban.ps1	success or wait	1	71E06A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0hiwndk4.bpq.psm1	success or wait	1	71E06A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_s4hshgl2.ban.ps1	0	1	31	1	success or wait	1	71E01B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0hiwndk4.bpq.psm1	0	1	31	1	success or wait	1	71E01B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 65 14 00 00 1b 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 fd 01 0a 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@ee@	success or wait	1	731876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 49 00 00 00 0e 00 20 00	H<@^L"My:I	success or wait	17	731876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	731876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	255	1	00		success or wait	11	731876FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	1168	4	00 08 00 03		success or wait	11	731876FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 fd 57 40 01 fd 10 40 01 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 68 38 40 01 67 38 40 01 10 6f 40 01 11 6f 40 01 42 4d 40 01 05 0e fd 00 fd 44 40 01 6d 45 40 01 45 4d 40 01 fd 71 40 01 fd 71 40 01 fd 53 40 01 fd 25 40 01 fd 6e 40 01 34 26 40	T@>@@V@H@X@[@ W@@NT@HT@S@S@ hT@S @S@S@\@T@T@@X @? X@T@S@S@T@T@xT @ zT@T@=M@DM@:M@" M@ M@!M@;M@D@D@ @M@<M@$M@8M@? M@h8@g8@o@o@BM @D@ mE@EM@q@q@S@% @n@4&@	success or wait	11	731876FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72E95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72DF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E9CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E9CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72DF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72DF03DE	ReadFile
stdin	unknown	1024	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	71E01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72DF03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72DF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	71E01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
stdin	unknown	1024	pipe broken	1	71E01B4F	ReadFile

Analysis Process: conhost.exe PID: **6816**, Parent PID: **6824**

General

Target ID:	2
Start time:	17:18:19
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
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: TrustedInstaller.exe PID: **6536**, Parent PID: **552**

General

Target ID:	4
Start time:	17:18:25
Start date:	06/06/2023
Path:	C:\Windows\servicing\TrustedInstaller.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\servicing\TrustedInstaller.exe
Imagebase:	0x7ff72a050000
File size:	131584 bytes
MD5 hash:	4578046C54A954C917BB393B70BA0AEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Analysis Process: file.exe PID: **1488**, Parent PID: **6760**

General

Target ID:	5
Start time:	17:18:26
Start date:	06/06/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	4377472 bytes

MD5 hash:	5E7D3490818E3F2A96F7A9DFC6950F9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000005.00000002.400548532.0000000000843000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000005.00000002.403769101.000000002BA3000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000005.00000002.400548532.0000000000400000.00000040.00000001.01000000.00000003.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000005.00000003.362103364.0000000003CD1000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000005.00000003.362103364.0000000003890000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000005.00000002.414419556.00000000033E3000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000005.00000002.414419556.0000000002FA0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\rss	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	465615	CreateDirectoryW
C:\Windows\rss\csrss.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	465615	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	86			invalid handle	4	465615	WriteFile
C:\Windows\rss\csrss.exe	0	32768	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 fd 3a 5d fd 5b 33 fd fd 5b 33 fd fd 5b 33 fd fd 09 fd fd fd 5b 33 fd fd 09 fd fd fd 5b 33 fd fd 09 fd fd fd 5b 33 fd fd fd 48 fd fd 5b 33 fd fd 5b 32 fd 3b 5b 33 fd fd 09 fd fd fd 5b 33 fd fd 09 fd fd fd 5b 33 fd fd 09 fd fd fd 5b 33 fd 52 69 63 68 fd 5b 33 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 85 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 09 00 00 fd 40	MZ@!L!This program cannot be run in DOS mode.$:][3[3[3[3[3[3 H[3[2; [3[3[3[3Rich[3PELc@	success or wait	134	465615	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\file.exe	0	96	success or wait	38	465615	ReadFile
C:\Users\user\Desktop\file.exe	unknown	4	success or wait	138	465615	ReadFile
\pipe	unknown	512	success or wait	48	465615	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\pipe	unknown	1497	pipe broken	4	465615	ReadFile
C:\Users\user\Desktop\file.exe	unknown	32768	end of file	1	465615	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths	C:\Windows\rss	dword	0	success or wait	1	465615	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\AppData\Local\Temp\csrss	dword	0	success or wait	1	465615	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths	C:\Windows\windefender.exe	dword	0	success or wait	1	465615	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths	C:\Windows\System32\drivers	dword	0	success or wait	1	465615	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes	csrss.exe	dword	0	success or wait	1	465615	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes	windefender.exe	dword	0	success or wait	1	465615	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes	file.exe	dword	0	success or wait	1	465615	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	csrss	unicode	"C:\Windows\rss\csrss.exe"	success or wait	1	465615	RegSetValueExW

Analysis Process: powershell.exe PID: **5576**, Parent PID: **1488**

General

Target ID:	6
Start time:	17:18:28
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xe60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71E0BEFF	CreateDirectoryW
C:\Windows\TEMP__PSscriptPolicyTest_txvnygx2.3pj.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71E01E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\TEMP__PSscriptPolicyTest_m40tnpqs.odn.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71E01E60	CreateFileW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72EBCF06	unknown
C:\Windows\SysWOW64\config\systemprofile\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	72EBCF06	unknown
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	73081926	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\Temp__PSscriptPolicyTest_txvnygx2.3pj.ps1	success or wait	1	71E06A95	DeleteFileW
C:\Windows\Temp__PSscriptPolicyTest_m40tnpqs.odn.psm1	success or wait	1	71E06A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp__PSscriptPolicyTest_txvnygx2.3pj.ps1	0	1	31	1	success or wait	1	71E01B4F	WriteFile
C:\Windows\Temp__PSscriptPolicyTest_m40tnpqs.odn.psm1	0	1	31	1	success or wait	1	71E01B4F	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 4a 14 00 00 1a 00 00 00 fd 0d fd 05 61 08 4f 08 4f 08 00 00 00 00 fd 01 2b 00 fd 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@eJaOO+@	success or wait	1	731876FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 49 00 00 00 0e 00 20 00	H<@^L"My:I	success or wait	17	731876FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	731876FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	255	1	00		success or wait	11	731876FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	1168	4	00 08 00 03		success or wait	11	731876FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 09 09 fd 00 5b 01 40 00 09 0c fd 00 58 64 40 01 56 64 40 01 fd 2a 40 01 fd 57 40 01 fd 10 40 01 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 45 4d 00 01 fd 71 00 01 fd 71 00	T@>@@V@H@X@[@Xd@Vd@*@W@@NT@HT@ S@S@hT@S@S@S@\ @T@T@@X@? X@T@S@S @T@T@xT@zT@T@= M@DM@:M@"M@ M@!M @;M@D@D@@M@<M @$M@8M? MBMDmEEMqq	success or wait	11	731876FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72E95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72DF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E9CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E9CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E9CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72E9CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	72E9CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	72E9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72DF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72DF03DE	ReadFile
stdin	unknown	1024	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72DF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
stdin	unknown	1024	pipe broken	1	71E01B4F	ReadFile

Analysis Process: conhost.exe PID: **5984**, Parent PID: **5576**

General	
Target ID:	7
Start time:	17:18:28
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **2760**, Parent PID: **1488**

General	
Target ID:	8
Start time:	17:18:35
Start date:	06/06/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Sysnative\cmd.exe /C "netsh advfirewall firewall add rule name="csrss" dir=in action=allow program="C:\Windows\rss\csrss.exe" enable=yes"
Imagebase:	0x7ff7651b0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: **3432**, Parent PID: **2760**

General	
Target ID:	9
Start time:	17:18:35
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: netsh.exe PID: **6792**, Parent PID: **2760**

General

Target ID:	10
Start time:	17:18:36
Start date:	06/06/2023
Path:	C:\Windows\System32\netsh.exe
Wow64 process (32bit):	false
Commandline:	netsh advfirewall firewall add rule name="csrss" dir=in action=allow program="C:\Windows\rss\csrss.exe" enable=yes
Imagebase:	0x7ff747c60000
File size:	92672 bytes
MD5 hash:	98CC37BBF363A38834253E22C80A8F32
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **7076**, Parent PID: **1488**

General

Target ID:	11
Start time:	17:18:36
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xe60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\TEMP__PSscriptPolicyTest_phccmwlw.m0k.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71E01E60	CreateFileW
C:\Windows\TEMP__PSscriptPolicyTest_ninjjd0h.sdc.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71E01E60	CreateFileW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72EBCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\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	72EBCF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\Temp__PSscriptPolicyTest_phccmwlw.m0k.ps1	success or wait	1	71E06A95	DeleteFileW
C:\Windows\Temp__PSscriptPolicyTest_ninjjd0h.sdc.psm1	success or wait	1	71E06A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp__PSscriptPolicyTest_phccmwlw.m0k.ps1	0	1	31	1	success or wait	1	71E01B4F	WriteFile
C:\Windows\Temp__PSscriptPolicyTest_ninjjd0h.sdc.psm1	0	1	31	1	success or wait	1	71E01B4F	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 4a 14 00 00 1a 00 00 00 fd 0d fd 05 61 08 4f 08 4f 08 00 00 00 00 fd 01 2b 00 fd 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@eJaOO+@	success or wait	1	731876FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 49 00 00 00 0e 00 20 00	H<@^L"My:I	success or wait	17	731876FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	731876FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	255	1	00		success or wait	11	731876FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	1168	4	00 08 00 03		success or wait	11	731876FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 09 09 fd 00 5b 01 40 00 09 0c fd 00 58 64 40 01 56 64 40 01 fd 2a 40 01 fd 57 40 01 fd 10 40 01 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 45 4d 00 01 fd 71 00 01 fd 71 00	T@>@@V@H@X@[@Xd@Vd@*@W@@NT@HT@ S@S@hT@S@S@S@\ @T@T@@X@? X@T@S@S @T@T@xT@zT@T@= M@DM@:M@"M@ M@!M @;M@D@D@@M@<M @$M@8M? MBMDmEEMqq	success or wait	11	731876FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72E95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72DF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E9CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E9CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72DF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Managemen t.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	72DF03DE	ReadFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Micro soft\Windows\PowerShell\StartupProfileData-Interactive	unknown	64	success or wait	1	72EA1F73	ReadFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Micro soft\Windows\PowerShell\StartupProfileData-Interactive	unknown	22236	success or wait	1	72EA203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuratio n.ni.dll.aux	unknown	864	success or wait	1	72DF03DE	ReadFile
stdin	unknown	1024	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Op eration.Validation.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Op eration.Validation.psd1	unknown	492	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Op eration.Validation.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psd1	unknown	4096	success or wait	2	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psm1	unknown	4096	success or wait	7	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psm1	unknown	682	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psm1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71E01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	117	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72DF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72E95705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
stdin	unknown	1024	pipe broken	1	71E01B4F	ReadFile

Analysis Process: conhost.exe PID: **6892**, Parent PID: **7076**

General

Target ID:	12
Start time:	17:18:36
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
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: **5848**, Parent PID: **1488**

General

Target ID:	13

Start time:	17:18:40
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xe60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71D65B28	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	71D65B28	unknown
C:\Windows\TEMP__PSscriptPolicyTest_5rosccoi.3tj.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71E01E60	CreateFileW
C:\Windows\TEMP__PSscriptPolicyTest_4kbnorl3.12h.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71E01E60	CreateFileW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72EBCF06	unknown
C:\Windows\SysWOW64\config\systemprofile\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	72EBCF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\Temp__PSscriptPolicyTest_5rosccoi.3tj.ps1	success or wait	1	71E06A95	DeleteFileW
C:\Windows\Temp__PSscriptPolicyTest_4kbnorl3.12h.psm1	success or wait	1	71E06A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp__PSscriptPolicyTest_5rosccoi.3tj.ps1	0	1	31	1	success or wait	1	71E01B4F	WriteFile
C:\Windows\Temp__PSscriptPolicyTest_4kbnorl3.12h.psm1	0	1	31	1	success or wait	1	71E01B4F	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 4a 14 00 00 1a 00 00 00 fd 0d fd 05 61 08 4f 08 4f 08 00 00 00 00 fd 01 2b 00 fd 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00	@eJaOO+@	success or wait	1	731876FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 49 00 00 00 0e 00 20 00	H<@^L"My:I	success or wait	17	731876FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	731876FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	255	1	00		success or wait	11	731876FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	1168	4	00 08 00 03		success or wait	11	731876FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 09 09 fd 00 5b 01 40 00 09 0c fd 00 58 64 40 01 56 64 40 01 fd 2a 40 01 fd 57 40 01 fd 10 40 01 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 45 4d 00 01 fd 71 00 01 fd 71 00	T@>@@V@H@X@[@Xd@Vd@*@W@@NT@HT@ S@S@hT@S@S@S@\ @T@T@@X@? X@T@S@S @T@T@xT@zT@T@= M@DM@:M@"M@ M@!M @;M@D@D@@M@<M @$M@8M? MBMDmEEMqq	success or wait	11	731876FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72E95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72DF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E9CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E9CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72DF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	72DF03DE	ReadFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	unknown	64	success or wait	1	72EA1F73	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72DF03DE	ReadFile
stdin	unknown	1024	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	115	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	71E01B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72DF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72DF03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72E95705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72E95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	71E01B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	71E01B4F	ReadFile
stdin	unknown	1024	pipe broken	1	71E01B4F	ReadFile

Analysis Process: conhost.exe PID: **3372**, Parent PID: **5848**

General

Target ID:	14
Start time:	17:18:40
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csrss.exe PID: **768**, Parent PID: **1488**

General

Target ID:	15
Start time:	17:18:44
Start date:	06/06/2023
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\rss\csrss.exe
Imagebase:	0x400000
File size:	4377472 bytes
MD5 hash:	5E7D3490818E3F2A96F7A9DFC6950F9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000F.00000002.624848873.0000000003400000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 0000000F.00000002.624848873.0000000003843000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 0000000F.00000002.615156234.0000000000400000.00000040.00000001.01000000.00000005.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000F.00000002.624483863.0000000003000000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 0000000F.00000003.401909888.0000000003CF0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 0000000F.00000002.615156234.0000000000843000.00000040.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 0000000F.00000003.401909888.0000000004131000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 76%, ReversingLabs

Analysis Process: powershell.exe PID: **7012**, Parent PID: **768**

General	
Target ID:	16
Start time:	17:18:46
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xe60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **6724**, Parent PID: **7012**

General	
Target ID:	17
Start time:	17:18:47
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5760**, Parent PID: **768**

General	
Target ID:	21
Start time:	17:18:56
Start date:	06/06/2023
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks /CREATE /SC ONLOGON /RL HIGHEST /TR "C:\Windows\rss\csrss.exe" /TN csrss /F
Imagebase:	0x7ff6d8c70000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csrss.exe PID: **6772**, Parent PID: **3320**

General	
Target ID:	22
Start time:	17:18:56
Start date:	06/06/2023
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true

Commandline:	"C:\Windows\rss\csrss.exe"
Imagebase:	0x400000
File size:	4377472 bytes
MD5 hash:	5E7D3490818E3F2A96F7A9DFC6950F9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000016.00000002.471247409.0000000003000000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000016.00000002.442933383.0000000000400000.00000040.00000001.01000000.00000005.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000016.00000002.442933383.0000000000843000.00000040.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000016.00000002.474423573.0000000003843000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000016.00000002.474423573.0000000003400000.00000040.00001000.00020000.00000000.sdmp, Author: unknown

Analysis Process: conhost.exe PID: **7136**, Parent PID: **5760**

General

Target ID:	23
Start time:	17:18:56
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **6852**, Parent PID: **768**

General

Target ID:	24
Start time:	17:18:56
Start date:	06/06/2023
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks /delete /tn ScheduledUpdate /f
Imagebase:	0x7ff6d8c70000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **240**, Parent PID: **6852**

General

Target ID:	25
Start time:	17:18:56
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
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: **2896**, Parent PID: **768**

General	
Target ID:	26
Start time:	17:18:56
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xe60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **5124**, Parent PID: **2896**

General	
Target ID:	27
Start time:	17:18:56
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csrss.exe PID: **2344**, Parent PID: **1100**

General	
Target ID:	28
Start time:	17:18:57
Start date:	06/06/2023
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\rss\csrss.exe
Imagebase:	0x400000
File size:	4377472 bytes
MD5 hash:	5E7D3490818E3F2A96F7A9DFC6950F9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 0000001C.00000002.599256866.0000000003843000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000001C.00000002.594116326.0000000003000000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 0000001C.00000002.566670417.0000000000843000.00000040.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 0000001C.00000002.566670417.0000000000400000.00000040.00000001.01000000.00000005.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000001C.00000002.599256866.0000000003400000.00000040.00001000.00020000.00000000.sdmp, Author: unknown

Analysis Process: cmd.exe PID: **2224**, Parent PID: **6772**

General	
Target ID:	29
Start time:	17:19:00
Start date:	06/06/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Sysnative\cmd.exe /C fodhelper
Imagebase:	0x7ff7651b0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4768**, Parent PID: **2224**

General	
Target ID:	30
Start time:	17:19:00
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: fodhelper.exe PID: **6780**, Parent PID: **2224**

General	
Target ID:	31
Start time:	17:19:00
Start date:	06/06/2023
Path:	C:\Windows\System32\fodhelper.exe
Wow64 process (32bit):	false
Commandline:	fodhelper
Imagebase:	0x7ff779cf0000
File size:	46080 bytes
MD5 hash:	1D1F9E564472A9698F1BE3F9FEB9864B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: fodhelper.exe PID: **4248**, Parent PID: **2224**

General	
Target ID:	32
Start time:	17:19:00
Start date:	06/06/2023
Path:	C:\Windows\System32\fodhelper.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\fodhelper.exe"
Imagebase:	0x7ff779cf0000
File size:	46080 bytes
MD5 hash:	1D1F9E564472A9698F1BE3F9FEB9864B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: fodhelper.exe PID: **6708**, Parent PID: **2224**

General	
Target ID:	37
Start time:	17:19:02
Start date:	06/06/2023
Path:	C:\Windows\System32\fodhelper.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\fodhelper.exe"
Imagebase:	0x7ff779cf0000
File size:	46080 bytes
MD5 hash:	1D1F9E564472A9698F1BE3F9FEB9864B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **1360**, Parent PID: **768**

General	
Target ID:	38
Start time:	17:19:02
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xe60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **5788**, Parent PID: **1360**

General	
Target ID:	39
Start time:	17:19:02
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csrss.exe PID: **5596**, Parent PID: **6708**

General

Target ID:	40
Start time:	17:19:03
Start date:	06/06/2023
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\rss\csrss.exe"
Imagebase:	0x400000
File size:	4377472 bytes
MD5 hash:	5E7D3490818E3F2A96F7A9DFC6950F9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000028.00000002.475119649.0000000000843000.00000040.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000028.00000002.510967623.0000000003000000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000028.00000002.514590108.0000000003843000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000028.00000002.514590108.0000000003400000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000028.00000002.475119649.0000000000400000.00000040.00000001.01000000.00000005.sdmp, Author: Florian Roth (Nextron Systems) • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000028.00000003.442621501.0000000003CF0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)

Analysis Process: csrss.exe PID: **5280**, Parent PID: **3320**

General

Target ID:	41
Start time:	17:19:04
Start date:	06/06/2023
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\rss\csrss.exe"
Imagebase:	0x400000
File size:	4377472 bytes
MD5 hash:	5E7D3490818E3F2A96F7A9DFC6950F9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000029.00000002.480076167.0000000000843000.00000040.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000029.00000002.517016941.0000000003843000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000029.00000002.480076167.0000000000400000.00000040.00000001.01000000.00000005.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000029.00000002.517016941.0000000003400000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000029.00000002.513462018.0000000003000000.00000040.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: powershell.exe PID: **1196**, Parent PID: **5596**

General

Target ID:	42
Start time:	17:19:06
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xe60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **6740**, Parent PID: **1196**

General

Target ID:	43
Start time:	17:19:06
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
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: **1364**, Parent PID: **2344**

General

Target ID:	44
Start time:	17:19:06
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xe60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **6720**, Parent PID: **1364**

General	
Target ID:	45
Start time:	17:19:14
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6104**, Parent PID: **5280**

General	
Target ID:	46
Start time:	17:19:14
Start date:	06/06/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Sysnative\cmd.exe /C fodhelper
Imagebase:	0x7ff7651b0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **6140**, Parent PID: **6104**

General	
Target ID:	47
Start time:	17:19:14
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: fodhelper.exe PID: **6048**, Parent PID: **6104**

General	
Target ID:	48
Start time:	17:19:15
Start date:	06/06/2023
Path:	C:\Windows\System32\fodhelper.exe

Wow64 process (32bit):	false
Commandline:	fodhelper
Imagebase:	0x7ff779cf0000
File size:	46080 bytes
MD5 hash:	1D1F9E564472A9698F1BE3F9FEB9864B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: fodhelper.exe PID: **5708**, Parent PID: **6104**

General	
Target ID:	49
Start time:	17:19:15
Start date:	06/06/2023
Path:	C:\Windows\System32\fodhelper.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\fodhelper.exe"
Imagebase:	0x7ff779cf0000
File size:	46080 bytes
MD5 hash:	1D1F9E564472A9698F1BE3F9FEB9864B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: fodhelper.exe PID: **6216**, Parent PID: **6104**

General	
Target ID:	53
Start time:	17:19:18
Start date:	06/06/2023
Path:	C:\Windows\System32\fodhelper.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\fodhelper.exe"
Imagebase:	0x7ff779cf0000
File size:	46080 bytes
MD5 hash:	1D1F9E564472A9698F1BE3F9FEB9864B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csrss.exe PID: **6316**, Parent PID: **5596**

General	
Target ID:	54
Start time:	17:19:18
Start date:	06/06/2023
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\rss\csrss.exe
Imagebase:	0x400000
File size:	4377472 bytes
MD5 hash:	5E7D3490818E3F2A96F7A9DFC6950F9C
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000036.00000002.509180776.0000000000400000.00000040.00000001.01000000.00000005.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000036.00000002.521380153.0000000003400000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000036.00000002.509180776.0000000000843000.00000040.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000036.00000002.521380153.0000000003843000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000036.00000002.518888987.0000000003000000.00000040.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: csrss.exe PID: **6464**, Parent PID: **6216**

General	
Target ID:	55
Start time:	17:19:19
Start date:	06/06/2023
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\rss\csrss.exe"
Imagebase:	0x400000
File size:	4377472 bytes
MD5 hash:	5E7D3490818E3F2A96F7A9DFC6950F9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000037.00000002.553779043.0000000003400000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000037.00000002.522989058.0000000000400000.00000040.00000001.01000000.00000005.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000037.00000002.548334385.0000000003000000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000037.00000002.522989058.0000000000843000.00000040.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000037.00000002.553779043.0000000003843000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: powershell.exe PID: **6652**, Parent PID: **6316**

General	
Target ID:	56
Start time:	17:19:22
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xe60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **6660**, Parent PID: **6652**

General	
Target ID:	57
Start time:	17:19:22
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
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: **4680**, Parent PID: **6464**

General

Target ID:	58
Start time:	17:19:25
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xe60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **4164**, Parent PID: **4680**

General

Target ID:	59
Start time:	17:19:25
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csrss.exe PID: **4472**, Parent PID: **6464**

General

Target ID:	60
Start time:	17:19:40
Start date:	06/06/2023
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\rss\csrss.exe
Imagebase:	0x400000
File size:	4377472 bytes
MD5 hash:	5E7D3490818E3F2A96F7A9DFC6950F9C
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 0000003C.00000002.570772687.0000000003843000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000003C.00000002.567142232.0000000003000000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 0000003C.00000002.555538595.0000000000400000.00000040.00000001.01000000.00000005.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 0000003C.00000002.555538595.0000000000843000.00000040.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000003C.00000002.570772687.0000000003400000.00000040.00001000.00020000.00000000.sdmp, Author: unknown

Analysis Process: powershell.exe PID: **2224**, Parent PID: **4472**

General	
Target ID:	61
Start time:	17:19:43
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xe60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **6532**, Parent PID: **2224**

General	
Target ID:	62
Start time:	17:19:44
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csrss.exe PID: **6216**, Parent PID: **2344**

General	
Target ID:	64
Start time:	17:19:59
Start date:	06/06/2023
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\rss\csrss.exe
Imagebase:	0x400000
File size:	4377472 bytes
MD5 hash:	5E7D3490818E3F2A96F7A9DFC6950F9C
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: 00000040.00000002.598741475.0000000000400000.00000040.00000001.01000000.00000005.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000040.00000002.604158371.0000000003000000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000040.00000002.609271972.0000000003400000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000040.00000002.609271972.0000000003843000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Glupteba, Description: Yara detected Glupteba, Source: 00000040.00000002.598741475.0000000000843000.00000040.00000001.01000000.00000005.sdmp, Author: Joe Security

Analysis Process: powershell.exe PID: **6184**, Parent PID: **6216**

General	
Target ID:	65
Start time:	17:20:04
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -nologo -noprofile
Imagebase:	0xe60000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **6200**, Parent PID: **6184**

General	
Target ID:	66
Start time:	17:20:04
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly