ID: 513164
Sample Name:
rzMvWQOGAE.bin
Cookbook: default.jbs
Time: 21:28:37
Date: 01/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

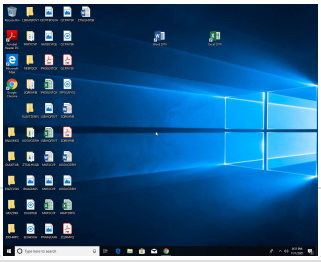
Windows Analysis Report rzMvWQOGAE.bin

Overview

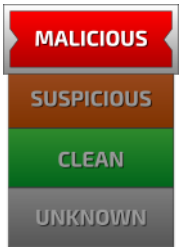
General Information

Sample Name:	rzMvWQOGAE.bin (renamed file extension from bin to exe)
Analysis ID:	513164
MD5:	d3c5b425a0e346..
SHA1:	347b3921b06609..
SHA256:	325ecd90ce19dd..
Tags:	exe Exmatter
Infos:	

Most interesting Screenshot:



Detection

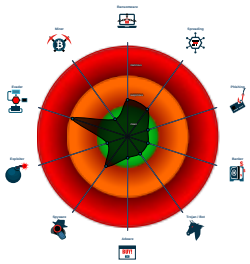


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Suspicious powershell command line…
- Deletes itself after installation
- Uses 32bit PE files
- Queries the volume information (nam…
- Yara signature match
- Very long cmdline option found, this…
- May sleep (evasive loops) to hinder …
- Uses code obfuscation techniques (…
- Detected potential crypto function
- Sample execution stops while proce…
- Contains long sleeps (>= 3 min)

Classification



Process Tree

- **System is w10x64**
- rzMvWQOGAE.exe (PID: 6232 cmdline: 'C:\Users\user\Desktop\rzMvWQOGAE.exe' MD5: D3C5B425A0E346AF5BD572BBC238CCBA)
  - conhost.exe (PID: 1236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6832 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -WindowStyle Hidden -C $path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Process | Where-Object {$_.Path -like $path} | Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path; MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6648 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -WindowStyle Hidden -C $path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Process | Where-Object {$_.Path -like $path} | Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path; MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6696 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -WindowStyle Hidden -C $path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Process | Where-Object {$_.Path -like $path} | Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path; MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6508 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 3084 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -WindowStyle Hidden -C $path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Process | Where-Object {$_.Path -like $path} | Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path; MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5296 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5956 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -WindowStyle Hidden -C $path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Process | Where-Object {$_.Path -like $path} | Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path; MD5: DBA3E6449E97D4E3DF64527EF7012A10)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
Process Memory Space: powershell.exe PID: 6832	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x280d1:$sa2: -encodedCommand • 0x280fd:$sa2: -encodedCommand • 0x287dc:$sa2: -EncodedCommand • 0x292fd:$sa2: -EncodedCommand • 0x29398:$sa2: -encodedCommand • 0x15031:$sb3: -WindowStyle Hidden • 0x1514d:$sb3: -WindowStyle Hidden • 0x1571a:$sb3: -WindowStyle Hidden • 0x4fab2:$sb3: -WindowStyle Hidden • 0x71fef:$sb3: -WindowStyle Hidden • 0x72798:$sb3: -WindowStyle Hidden • 0x75ebf:$sb3: -WindowStyle Hidden • 0x285c4:$sc2: -NoProfile • 0x28605:$sd2: -NonInteractive
Process Memory Space: powershell.exe PID: 6648	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0xbb053:$sa2: -encodedCommand • 0xbb07f:$sa2: -encodedCommand • 0xbb75e:$sa2: -EncodedCommand • 0xbc27f:$sa2: -EncodedCommand • 0xbc31a:$sa2: -encodedCommand • 0x1d99:$sb3: -WindowStyle Hidden • 0x1eb5:$sb3: -WindowStyle Hidden • 0x25aa:$sb3: -WindowStyle Hidden • 0x292d:$sb3: -WindowStyle Hidden • 0x2f78:$sb3: -WindowStyle Hidden • 0x46483:$sb3: -WindowStyle Hidden • 0x19db59:$sb3: -WindowStyle Hidden • 0xbb546:$sc2: -NoProfile • 0xbb587:$sd2: -NonInteractive

Sigma Overview

System Summary:

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Data Obfuscation:

Suspicious powershell command line found

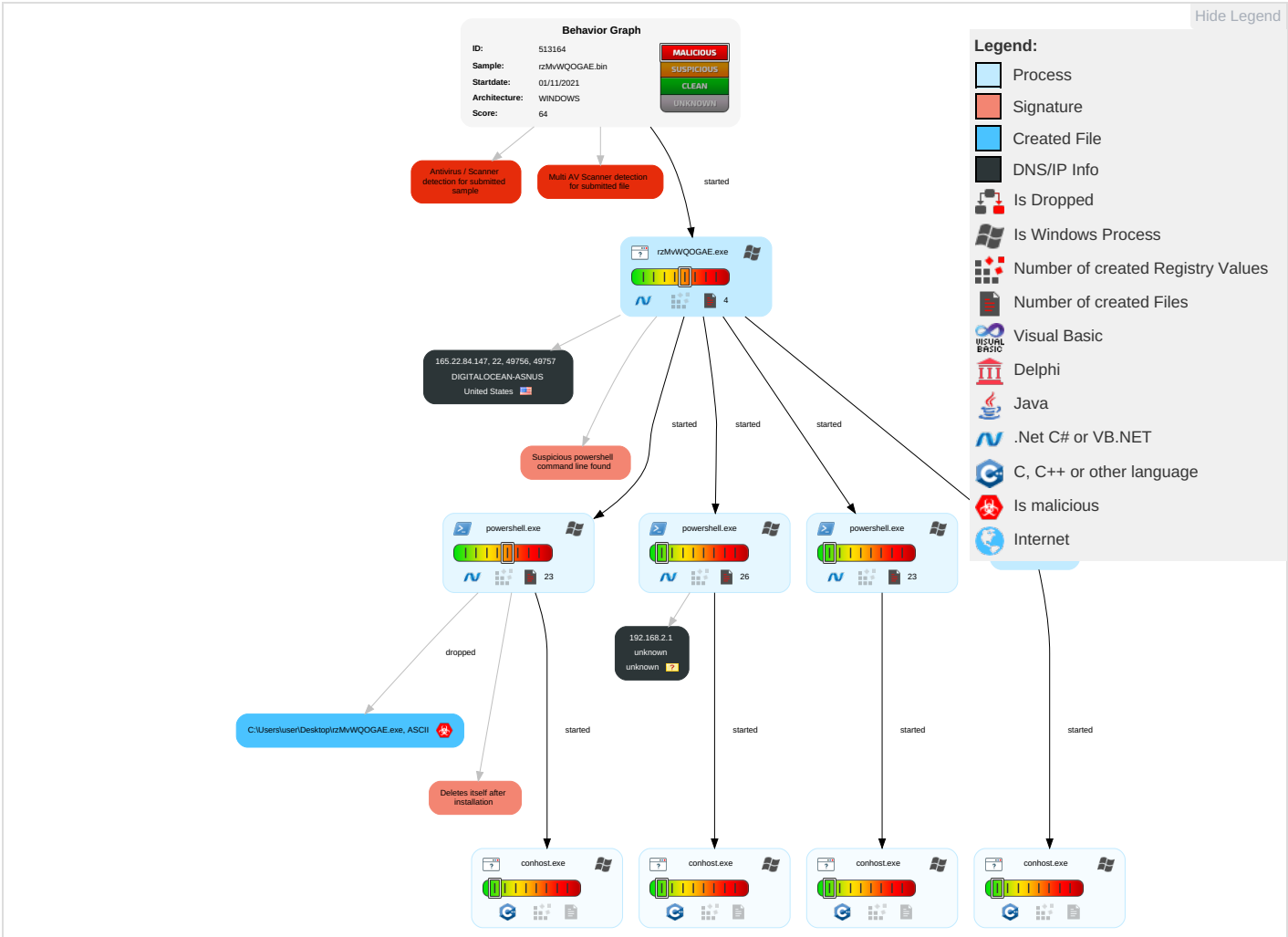
Hooking and other Techniques for Hiding and Protection:

Deletes itself after installation

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Command and Scripting Interpreter 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	PowerShell 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

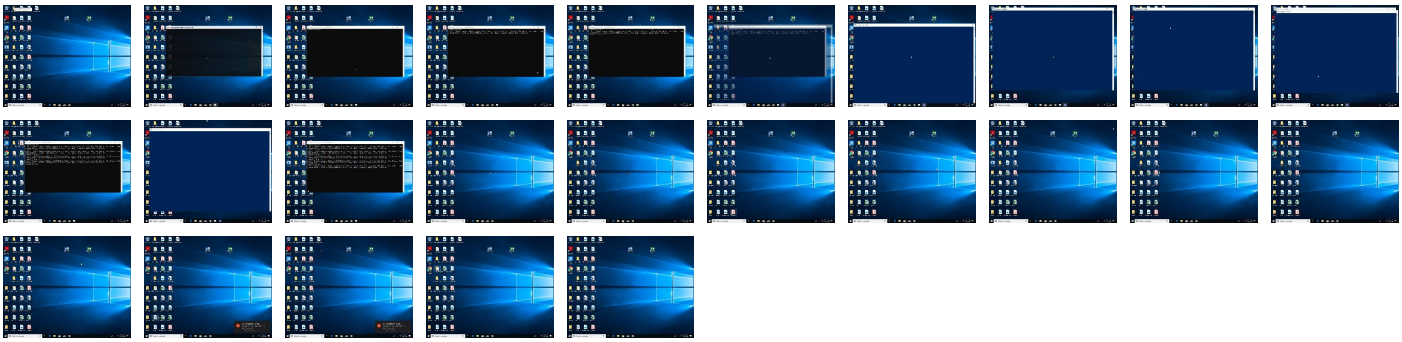
Behavior Graph



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
rzMvWQOGAE.exe	17%	Metadefender		Browse
rzMvWQOGAE.exe	68%	ReversingLabs	ByteCode-MSIL.Ransomware.BlackMatter	
rzMvWQOGAE.exe	100%	Avira	TR/Kryptik.uoskd	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
165.22.84.147	unknown	United States		14061	DIGITALOCEAN-ASNUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	513164
Start date:	01.11.2021
Start time:	21:28:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	rzMvWQOGAE.bin (renamed file extension from bin 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:	29
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:	mal64.winEXE@16/28@0/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 12.5% (good quality ratio 7.3%) • Quality average: 32.7% • Quality standard deviation: 34.8%
HCA Information:	• Successful, ratio: 98% • 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
21:30:00	API Interceptor	133x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	JSUAd0NPag.exe	Get hash	malicious	Browse	• 157.230.28.192
	gqTrv5VEem.exe	Get hash	malicious	Browse	• 159.89.128.13
	SecuriteInfo.com.Suspicious.Win32.Save.a.4727.dll	Get hash	malicious	Browse	• 104.248.15 5.133
	SecuriteInfo.com.Suspicious.Win32.Save.a.31095.dll	Get hash	malicious	Browse	• 104.248.15 5.133
	SecuriteInfo.com.Suspicious.Win32.Save.a.28634.dll	Get hash	malicious	Browse	• 104.248.15 5.133
	SecuriteInfo.com.Suspicious.Win32.Save.a.12010.dll	Get hash	malicious	Browse	• 104.248.15 5.133
	SecuriteInfo.com.Malware.Heuristic.1001.8375.dll	Get hash	malicious	Browse	• 104.248.15 5.133
	SecuriteInfo.com.Suspicious.Win32.Save.a.4798.dll	Get hash	malicious	Browse	• 104.248.15 5.133
	SecuriteInfo.com.Suspicious.Win32.Save.a.4727.dll	Get hash	malicious	Browse	• 104.248.15 5.133
	SecuriteInfo.com.Suspicious.Win32.Save.a.31095.dll	Get hash	malicious	Browse	• 104.248.15 5.133
	SecuriteInfo.com.Suspicious.Win32.Save.a.28634.dll	Get hash	malicious	Browse	• 104.248.15 5.133
	SecuriteInfo.com.Suspicious.Win32.Save.a.12010.dll	Get hash	malicious	Browse	• 104.248.15 5.133
	SecuriteInfo.com.Malware.Heuristic.1001.8375.dll	Get hash	malicious	Browse	• 104.248.15 5.133

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Suspicious.Win32.Save.a.4798.dll	Get hash	malicious	Browse	• 104.248.155.133
	SecuriteInfo.com.Suspicious.Win32.Save.a.6275.dll	Get hash	malicious	Browse	• 104.248.155.133
	SecuriteInfo.com.Suspicious.Win32.Save.a.4037.dll	Get hash	malicious	Browse	• 104.248.155.133
	SecuriteInfo.com.Suspicious.Win32.Save.a.29964.dll	Get hash	malicious	Browse	• 104.248.155.133
	SecuriteInfo.com.Suspicious.Win32.Save.a.6275.dll	Get hash	malicious	Browse	• 104.248.155.133
	SecuriteInfo.com.Suspicious.Win32.Save.a.4037.dll	Get hash	malicious	Browse	• 104.248.155.133
	SecuriteInfo.com.Suspicious.Win32.Save.a.29964.dll	Get hash	malicious	Browse	• 104.248.155.133

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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):	8003
Entropy (8bit):	4.839308921501875
Encrypted:	false
SSDEEP:	192:yxoe5oVsm5emdVVFn3eGOVpN6K3bkkjo59gkjDt4iWN3yBGHh9smidcU6CXpOTik:DBVoGIpN6KQkj2Wkjh4iUx0mib4J
MD5:	937C6E940577634844311E349BD4614D
SHA1:	379440E933201CD3E6E6BF9B0E61B7663693195F
SHA-256:	30DC628AB2979D2CF0D281E998077E5721C68B9BBA61610039E11FDC438B993C
SHA-512:	6B37FE533991631C8290A0E9CC0B4F11A79828616BEF0233B4C57EC7C9DCBFC274FB7E50FC920C4312C93E74CE621B6779F10E4016E9FD794961696074BDFBF/
Malicious:	false
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:	modified
Size (bytes):	18620
Entropy (8bit):	5.597775927141057
Encrypted:	false
SSDEEP:	384:FtpPXWzEKe7bX88ESBKnR0jul/779bLfcQ/Ic5cTY8n:h724KR0Cl5RjNu
MD5:	5E1D030CA67A33157CDB599E11A2E684
SHA1:	90F9CCD20E9157D720D19ED6656FD3752E26F0E9
SHA-256:	0FB7212A524DD3D4C6A05EC6FBD7E4D06FE7C0C6ECC76BC3DA9778473101E728
SHA-512:	579392ED74384C796E624E39106E259EF46AE583EFC7C61E144D14DDB3571670DE7D09647BF1B3084AD524F94BEC491B8D37C14C8E5D76A709DB38AF1276DB3
Malicious:	false
Preview:	@...e.....d...~.{.....<.4.....@.....H.....<@.^.L."My...:'..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)U.....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.<.....):gK..G...$.1.q.....System.ConfigurationH..... ....H..m)aUu.....Microsoft.Powe rShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.P.....-K..s.F..*.]`.,(.....(.Microsoft.PowerShell.Commands.ManagementD.....-.D.F.<;.nt.1. .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1gegaynp.l4w.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
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_1tmrxd4d.uxh.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
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3yos1554.31w.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
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5pws0tqn.3me.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
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cocmpo00.ljs.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
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_eqnwawwy.wpo.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
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\FRQ4T5NV3HSHD639O02M.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6208
Entropy (8bit):	3.7617465135135184
Encrypted:	false
SSDEEP:	96:y50ceEwuCN9yP9SkvhkvCCtJVrZeHgyaZeHgy2:mNeE4WgJVr5ya5y2
MD5:	C92005C06D1EFF9C3C69A0E999612EE7
SHA1:	5A5FE37AE96D4CAF3EEF2E9C9D87E09248658ECB
SHA-256:	FB3AD03EC3D022C3792A59A0BE3EE06625869A2BCCA3F0BDCB9188D19C835203
SHA-512:	130F84EED060DF004BE1B0A6FBA52F0D5B1E6A64898E6FA6CE06245790857EC2E8D5917BE216C1E1E517409C3C1F2E36CCA27D3BCB3AB6D7C162D5E2CA518 A7
Malicious:	false
Preview:	.....FL.....F.".. ...'+k.!-...V...a..\.....:..DG..Yr?.D..U..k0.&...&.....d.!-..rw.&>....SkH.....t...CFSF..1.....N....AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....N..bS.#.....Y.....t..A.p.p.D.a.t.a...B.V.1.....N....Roaming.@.....N..bS.#.....Y.....D...R.o.a.m.i.n.g.....\.1.....>Q.z..MICROS~1..D. .....N..bS.#.....Y....._..M.i.c.r.o.s.o.f.t.....V.1.....>Qc{..Windows.@.....N..bS.#.....Y.....I..W.i.n.d.o.w.s.....1.....N....STARTM~1..n.....N..bS.#.....Y..... .....D.....G`..S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....1.....P%v..Programs..j.....N..bS.#.....Y.....@.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .7.8.2.....n.1.....L...WINDOW~1..V.....N..bS.#.....Y.....T_..W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....z.2.....L.. .WINDOW~1.LNK..^.....N...Px.....Y.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\QFDFMM8ZPLCBKUCHCMRQ.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6208
Entropy (8bit):	3.7635933226544913
Encrypted:	false
SSDEEP:	96:y5keEwuCN9yP9SkvhkvCCtJVrZeHgyaZeHgy2:mkeE4WgJVr5ya5y2
MD5:	DF4E9B69DD764D99F7CF85B05CDD4ADE
SHA1:	CEE1061B8982D724AA1A7116DA9406518161F310
SHA-256:	C7C2D9E0F3520A76C5A260425F945E5AB03FA758C55C1C45B8FB44E1977B8CE2
SHA-512:	929AE2395502280404B032C34891C72EDC1345DF8665D23538C1C7C60BC5227F4B44F92FC492BF3CEEDEED7858B90F703E43871D184EA55E6EA64CC73D37A07
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\QFDFMM8ZPLCBKUCHCMRQ.temp	
Preview:	.....FL.....F."... ...'+k.!-...V...a..\.....:..DG..Yr?.D..U..k0.&...&.....d.!-..rw.&>.....J.....t...CFSF..1.....N....AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....N..bS.#.....Y.....t..A.p.p.D.a.t.a...B.V.1.....N....Roaming.@.....N..bS.#.....Y.....D...R.o.a.m.i.n.g.....\.1.....>Q.z..MICROS~1..D. .....N..bS.#.....Y....._..M.i.c.r.o.s.o.f.t.....V.1.....>Qc{..Windows.@.....N..bS.#.....Y.....I..W.i.n.d.o.w.s.....1.....N....STARTM~1..n.....N..bS.#.....Y..... .....D.....G`..S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.6.....1.....P%v..Programs..j.....N..bS.#.....Y.....@.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1 .7.8.2.....n.1.....L...WINDOW~1..V.....N..bS.#.....Y.....T_..W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....z.2.....L.. .WINDOW~1.LNK..^.....N...Px.....Y.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\VCEOL5MDX8L2VA4M3TY3.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6208
Entropy (8bit):	3.76302741289499
Encrypted:	false
SSDEEP:	96:y5KeEwuCN9KP9SkvhkvCCtJVrZeHgyaZeHgy2:mKeE4OgJVr5ya5y2
MD5:	93C45B56B18A853486BCB9CC1E5ADD75
SHA1:	A63DB5831B55973ED1E1C436E9BD47C04F4F6818
SHA-256:	5F3A0DF7DD09B7FC57EEE16D07F623241920B748E1B5EAA528D30524613C8D4E
SHA-512:	2BF9B939F4F6C1CBCE02428FAE50C3AB8F08FE18F3A1079DD10B2BEE84CF098463B346D3A9A2020B3CE857E84683C0B121498342C60134A4A806CBD54C2D93D B
Malicious:	false
Preview:	.....FL.....F."... ...'+k.!-...V...a..\.....:..DG..Yr?.D..U..k0.&...&.....d.!-..rw.&>....H.F.....t...CFSF..1.....N....AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....N..bS.#.....Y.....t..A.p.p.D.a.t.a...B.V.1.....N....Roaming.@.....N..bS.#.....Y.....D...R.o.a.m.i.n.g.....\.1.....>Q.z..MICROS~1..D. .....N..bS.#.....Y....._..M.i.c.r.o.s.o.f.t.....V.1.....>Qc{..Windows.@.....N..bS.#.....Y.....I..W.i.n.d.o.w.s.....1.....N....STARTM~1..n.....N..bS.#.....Y..... .....D.....G`..S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.6.....1.....P%v..Programs..j.....N..bS.#.....Y.....@.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1 .7.8.2.....n.1.....L...WINDOW~1..V.....N..>Q.y.....Y.....T_..W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....z.2.....L.. .WINDOW~1.LNK..^.....N...Px.....Y.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\YNPMUSIXEREMQWMKT0C4.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6208
Entropy (8bit):	3.7620548230400495
Encrypted:	false
SSDEEP:	96:y5d7eEwuCN9yP9SkvhkvCCtJVrZeHgyaZeHgy2:md7eE4WgJVr5ya5y2
MD5:	859EC29AC9F2456FFF9677DFB5386FF7
SHA1:	46EBC364EBFD516C28F015889E881367DBA23109
SHA-256:	F9B5C0512D493650E9B3A0334A937813D145D72CCD615BC32EFB044CC4463FAC
SHA-512:	5422C31AE22B2224CE3215D1EF070DC475302E8C5534EC3F4D00A87EFBB66C965C5AD9FEE34D5C3A0E8472E2CEADD050A751E2A9E66769B5C757C681BCC674 AC
Malicious:	false
Preview:	.....FL.....F."... ...'+k.!-...V...a..\.....:..DG..Yr?.D..U..k0.&...&.....d.!-..rw.&>....1.L.....t...CFSF..1.....N....AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....N..bS.#.....Y.....t..A.p.p.D.a.t.a...B.V.1.....N....Roaming.@.....N..bS.#.....Y.....D...R.o.a.m.i.n.g.....\.1.....>Q.z..MICROS~1..D. .....N..bS.#.....Y....._..M.i.c.r.o.s.o.f.t.....V.1.....>Qc{..Windows.@.....N..bS.#.....Y.....I..W.i.n.d.o.w.s.....1.....N....STARTM~1..n.....N..bS.#.....Y..... .....D.....G`..S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.6.....1.....P%v..Programs..j.....N..bS.#.....Y.....@.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1 .7.8.2.....n.1.....L...WINDOW~1..V.....N..bS.#.....Y.....T_..W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....z.2.....L.. .WINDOW~1.LNK..^.....N...Px.....Y.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms (copy)	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6208
Entropy (8bit):	3.7620548230400495
Encrypted:	false
SSDEEP:	96:y5d7eEwuCN9yP9SkvhkvCCtJVrZeHgyaZeHgy2:md7eE4WgJVr5ya5y2
MD5:	859EC29AC9F2456FFF9677DFB5386FF7
SHA1:	46EBC364EBFD516C28F015889E881367DBA23109
SHA-256:	F9B5C0512D493650E9B3A0334A937813D145D72CCD615BC32EFB044CC4463FAC
SHA-512:	5422C31AE22B2224CE3215D1EF070DC475302E8C5534EC3F4D00A87EFBB66C965C5AD9FEE34D5C3A0E8472E2CEADD050A751E2A9E66769B5C757C681BCC674 AC
Malicious:	false
Preview:	.....FL.....F."... ...'+k.!-...V...a..\.....:..DG..Yr?.D..U..k0.&...&.....d.!-..rw.&>....1.L.....t...CFSF..1.....N....AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....N..bS.#.....Y.....t..A.p.p.D.a.t.a...B.V.1.....N....Roaming.@.....N..bS.#.....Y.....D...R.o.a.m.i.n.g.....\.1.....>Q.z..MICROS~1..D. .....N..bS.#.....Y....._..M.i.c.r.o.s.o.f.t.....V.1.....>Qc{..Windows.@.....N..bS.#.....Y.....I..W.i.n.d.o.w.s.....1.....N....STARTM~1..n.....N..bS.#.....Y..... .....D.....G`..S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.8.6.....1.....P%v..Programs..j.....N..bS.#.....Y.....@.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1 .7.8.2.....n.1.....L...WINDOW~1..V.....N..bS.#.....Y.....T_..W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....z.2.....L.. .WINDOW~1.LNK..^.....N...Px.....Y.....

<table>
<tr><th colspan="2">C:\Users\user\Desktop\rzMvWQOGAE.exe</th></tr>
<tr><td>Process:</td><td>C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe</td></tr>
<tr><td>File Type:</td><td>ASCII text, with CRLF line terminators</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>196608</td></tr>
<tr><td>Entropy (8bit):</td><td>1.584962500721156</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>12:bGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGGt:n</td></tr>
<tr><td>MD5:</td><td>27D42E77774A19AA669EA688B0DBCF99</td></tr>
<tr><td>SHA1:</td><td>AE7DFD50822C31989B20FCC6A40BFA05CB46FBE6</td></tr>
<tr><td>SHA-256:</td><td>E93A2E475DA7CA7A3C01F7185E15B74262F83A79682F32DBB7046BF395DF2CD7</td></tr>
<tr><td>SHA-512:</td><td>0FE5C8DB92DA55EECDB68E21D3A20BDE8043CD2D65F3C699C168F85C433C03B1D727EF73AEED849DA37F06628323D6DBD7171CFFA795FCC2FF72CDD047B9
CB</td></tr>
<tr><td>Malicious:</td><td>true</td></tr>
<tr><td>Preview:</td><td>0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0.
.0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0
..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..
0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0.
.0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0..0</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\Documents\20211101\PowerShell_transcript.960781.1yjAoh6+.20211101212951.txt</th></tr>
<tr><td>Process:</td><td>C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe</td></tr>
<tr><td>File Type:</td><td>UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>1376</td></tr>
<tr><td>Entropy (8bit):</td><td>5.350148850304876</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24:BxSAC7vBVL7Qcx2DOXUWRTgaW8lS5cuLWdHjeTKKjX4CIym1ZJXIagaW8lS5cuFc:BZqvTLkcoOx8aP7uidqDYB1ZgaP7uZZ2</td></tr>
<tr><td>MD5:</td><td>E947343C63628A8A64D0BB50637F3429</td></tr>
<tr><td>SHA1:</td><td>B81C50927FC7E10F642F237B2182784B6F4E2730</td></tr>
<tr><td>SHA-256:</td><td>0D112FDDEB322BA11196FDB42FBE0F472DD3270EB4D183CFFC0985E76DB0FA28</td></tr>
<tr><td>SHA-512:</td><td>B5CBD555DFDA411BD678BE4FFAD23227FEB1216A5F6BC302BA1094E8DAFE150DBC2AB9D39616AC6AB1E3B9DE8314FEE40C050D9FA304D920B9A947D4C4D9
9AE</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.**********************..Windows PowerShell transcript start..Start time: 20211101213013..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 960781 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden -C $pat h = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Process | Where-Object {$_.Path -like $path} | Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Con tent -Path $path -Value $arr;Remove-Item -Path $path;..Process ID: 6832..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1. .**********************..**********************..Command start time: 20211101213014..**********************..PS>$path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Proce</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\Documents\20211101\PowerShell_transcript.960781.5ETV8bU+.20211101213002.txt</th></tr>
<tr><td>Process:</td><td>C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe</td></tr>
<tr><td>File Type:</td><td>UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>1376</td></tr>
<tr><td>Entropy (8bit):</td><td>5.3515816368710345</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>24:BxSATy7vBVL7Qcx2DOXUWRTgaW8lS5cuLW1HjeTKKjX4CIym1ZJXzagaW8lS5cuU:BZ+vTLkcoOx8aP7ui1qDYB1ZFaP7u9Zk</td></tr>
<tr><td>MD5:</td><td>82CF6A757334E79E94AA212F326DF5C2</td></tr>
<tr><td>SHA1:</td><td>3085CEDECF530F83E43CFED3D40C7263ABFE67F2</td></tr>
<tr><td>SHA-256:</td><td>D6B06A3080915970FD5948E6E6F8CEE5FBD05B6FD555F54CE50A3FCF9395BFC0</td></tr>
<tr><td>SHA-512:</td><td>F2ACE49581D91B67693D043EBCA8C044DE8975C51E63996E051E4A0A5747AE4884587EB254A055AA1D9924B8297467753290D096F1AD78C0643C41DB2DA8B58F</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Preview:</td><td>.**********************..Windows PowerShell transcript start..Start time: 20211101213004..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 960781 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden -C $pat h = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Process | Where-Object {$_.Path -like $path} | Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Con tent -Path $path -Value $arr;Remove-Item -Path $path;..Process ID: 3084..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1. .**********************..**********************..Command start time: 20211101213004..**********************..PS>$path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Proce</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\Documents\20211101\PowerShell_transcript.960781.MxEjtLZ+.20211101212958.txt</th></tr>
<tr><td>Process:</td><td>C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe</td></tr>
<tr><td>File Type:</td><td>UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>7194</td></tr>
<tr><td>Entropy (8bit):</td><td>5.404402535175835</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
</table>

C:\Users\user\Documents\20211101\PowerShell_transcript.960781.MxEjtLZ+.20211101212958.txt

SSDEEP:	192:PRsllkXJRJlkX0lk1dlk1dlkZXRi6A+96AzYtn6Z6AzYtn6Z6cYtn6P:P0eJve0mdmdwXBApAct6gAct6gXt6P
MD5:	1783F59AB25B342B36E02C5B78003B85
SHA1:	BDEB4978F3D546FDC257A878346206E2FE7F02F7
SHA-256:	948B7983F64483FD72318533CAB77EDEDDC8F53ABCD0365C61415EB0B67CE414
SHA-512:	D69536A18C0D88FBB6AC4D6828B1C9D82AF4117AB0776A6CD38D0DE77CF302471959B9A8341EBA080ED6400360F0D876D463B5D9602F9AD856411EE52A6B5C7
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20211101213000..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 960781 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden -C $path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Process \| Where-Object {$_.Path -like $path} \| Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path;..Process ID: 6696..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1. .**********************..**********************..Command start time: 20211101213000..**********************..PS>$path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Proce

C:\Users\user\Documents\20211101\PowerShell_transcript.960781.TkSD6WsL.20211101212959.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1376
Entropy (8bit):	5.354754558996781
Encrypted:	false
SSDEEP:	24:BxSAQ7vBVL7Qcx2DOXUWRTgaW8lS5cuLWMHjeTKKjX4CIym1ZJXIqagaW8lS5cuC:BZUvTLkcoOx8aP7uiMqDYB1ZuYaP7uZc
MD5:	876F4A66BBFC361FC396ABD6CB6B5322
SHA1:	AA87E7CEF4A0625AD8EF6DE8FDFB6E8988EA79F5
SHA-256:	5092FCDA0B1EB7EBC3450A4441DD2BEDCC2624D3AF8778EADE5D1299A01F8EBE
SHA-512:	67BC2B1000D5671A8A29E1743D2639EE93AA405241BB895669C0092ED6C9D980737724D7E88F33A57B0200AD51284E2F90EA1413E59869A7F8E6C742F90D8FCA
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20211101213019..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 960781 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden -C $path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Process \| Where-Object {$_.Path -like $path} \| Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path;..Process ID: 6648..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1. .**********************..**********************..Command start time: 20211101213019..**********************..PS>$path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Proce

\Device\ConDrv

Process:	C:\Users\user\Desktop\rzMvWQOGAE.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1230
Entropy (8bit):	5.125494385697167
Encrypted:	false
SSDEEP:	24:LgaW8lS5cuHgaW8lS5cuHgaW8lS5cuHgaW8lS5cuHgaW8lS5cuD:UaP7uAaP7uAaP7uAaP7uAaP7uD
MD5:	C87D5C270A46C3C6EDA9EAE6FF82358F
SHA1:	54E51FCEDB47A9FDA1F6BF6E0E283A1E520CBA62
SHA-256:	015A7A2266A4ACD84D6877F15153F3EBB8CBDFA721DEBD9DA9D19C18B40BB2F3
SHA-512:	B64659B73D1286BC465F337E1C58E08EC7D9B92A9608AB0CE606BAD9132540882AB0A3AA93BB6442D2005335EADC2FBCE3681700E75E88EFE07026ABF89C1A7 D
Malicious:	false
Preview:	Connecting to host.....$path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Process \| Where-Object {$_.Path -like $path} \| Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path;..Connecting to host.....$path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Process | Where-Object {$_.Path -like $path} \| Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path;..Connecting to host.....$path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Process | Where-Object {$_.Path -like $path} \| Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path;..Connecting to host.....$path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Process | Where-Object {$_.Path -like $path} \| Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path;..Connecting to ho

Static File Info

General

File type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.985282854254978

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	rzMvWQOGAE.exe
File size:	1857024
MD5:	d3c5b425a0e346af5bd572bbc238ccba
SHA1:	347b3921b0660986bc0ce4d1a41aa77f04377a37
SHA256:	325ecd90ce19dd8d184ffe7dfb01b0dd02a77e9eabcb587f3738bcfbd3f832a1
SHA512:	b1734c9eec4de9abbc31f298fa87b22805f1abc09fe2912969ae8644d900ebbe78d269fe0f4851f3bda62f27ce2c63b3ee454ae405e248bb06182183d2abdac7
SSDEEP:	24576:hM1fTF/NfFqf6r7LVhpPZxT1xtbzBHf8LAeqfk:hM1h+uhXpk
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....6a.....L.....>j... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x5c6a3e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6136E6F1 [Tue Sep 7 04:13:37 2021 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

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1c4a44	0x1c4c00	False	0.428841972667	data	5.98622952842	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x1c8000	0x596	0x600	False	0.41015625	data	4.03543885017	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1ca000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

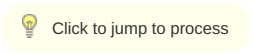
Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: rzMvWQOGAE.exe PID: 6232 Parent PID: 5416

General

Start time:	21:29:37
Start date:	01/11/2021
Path:	C:\Users\user\Desktop\rzMvWQOGAE.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\rzMvWQOGAE.exe'
Imagebase:	0xd40000
File size:	1857024 bytes
MD5 hash:	D3C5B425A0E346AF5BD572BBC238CCBA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 1236 Parent PID: 6232

General

Start time:	21:29:38
Start date:	01/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 6832 Parent PID: 6232

General

Start time:	21:29:46
Start date:	01/11/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -WindowStyle Hidden -C $path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Process \| Where-Object {$_.Path -like $path} \| Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path;
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6860 Parent PID: 6832

General

Start time:	21:29:48
Start date:	01/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

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

Analysis Process: powershell.exe PID: 6648 Parent PID: 6232

General

Start time:	21:29:51
Start date:	01/11/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -WindowStyle Hidden -C $path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Process \| Where-Object {$_.Path -like $path} \| Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path;
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6500 Parent PID: 6648

General

Start time:	21:29:51
Start date:	01/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 6696 Parent PID: 6232

General

Start time:	21:29:55
Start date:	01/11/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -WindowStyle Hidden -C $path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Process \| Where-Object {$_.Path -like $path} \| Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path;
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6508 Parent PID: 6696

General

Start time:	21:29:56
Start date:	01/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 3084 Parent PID: 6232

General

Start time:	21:29:59
Start date:	01/11/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -WindowStyle Hidden -C $path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Process \| Where-Object {$_.Path -like $path} \| Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path;
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 5296 Parent PID: 3084

General

Start time:	21:30:00
Start date:	01/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 5956 Parent PID: 6232

General

Start time:	21:30:03
Start date:	01/11/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' -WindowStyle Hidden -C $path = 'C:\Users\user\Desktop\rzMvWQOGAE.exe';Get-Process \| Where-Object {$_.Path -like $path} \| Stop-Process -Force;[byte[]]$arr = new-object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path $path;
Imagebase:	
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis