ID: 526642
Sample Name: malware.ps1
Cookbook: default.jbs
Time: 20:41:40
Date: 22/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

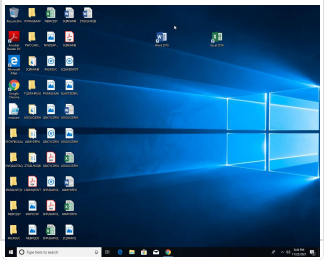
Windows Analysis Report malware.ps1

Overview

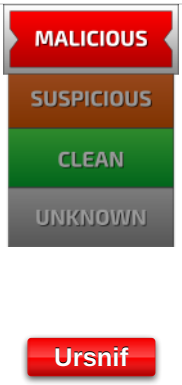
General Information

Sample Name:	malware.ps1
Analysis ID:	526642
MD5:	b0b0657a4c375c..
SHA1:	580152e7c431a4..
SHA256:	061eb7119db999..
Infos:	

Most interesting Screenshot:



Detection

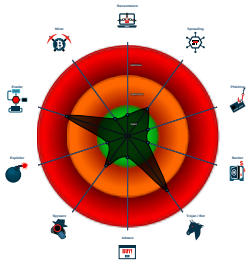


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Ursnif
- Compiles code for process injection …
- Sigma detected: Suspicious Csc.ex…
- Found a high number of Window / Us…
- Queries the volume information (nam…
- Drops PE files
- May sleep (evasive loops) to hinder …
- Compiles C# or VB.Net code
- Found dropped PE file which has no…
- Creates a process in suspended mo…
- Contains long sleeps (>= 3 min)
- Enables debug privileges

Classification



Process Tree

- **System is w10x64**
- powershell.exe (PID: 5416 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noLogo -ExecutionPolicy unrestricted -file "C:\Users\user\Desktop\malware.ps1 MD5: 95000560239032BC68B4C2FDFCDEF913)
  - conhost.exe (PID: 352 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - csc.exe (PID: 6196 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\ad403csv\ad403csv.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
    - cvtres.exe (PID: 6324 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESD522.tmp" "c:\Users\user\AppData\Local\Temp\ad403csv\CSCD6795C79BDE3450B9F7CAA8771DF83B.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
  - csc.exe (PID: 6408 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\5z3xaygo\5z3xaygo.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
    - cvtres.exe (PID: 6424 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESE4F1.tmp" "c:\Users\user\AppData\Local\Temp\5z3xaygo\CSC84083F42CE6043C2AA7FFF454285CD95.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.393533159.0000014F2E95C000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Process Memory Space: powershell.exe PID: 5416	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

HIPS / PFW / Operating System Protection Evasion:

Compiles code for process injection (via .Net compiler)

Stealing of Sensitive Information:

Yara detected Ursnif

Remote Access Functionality:

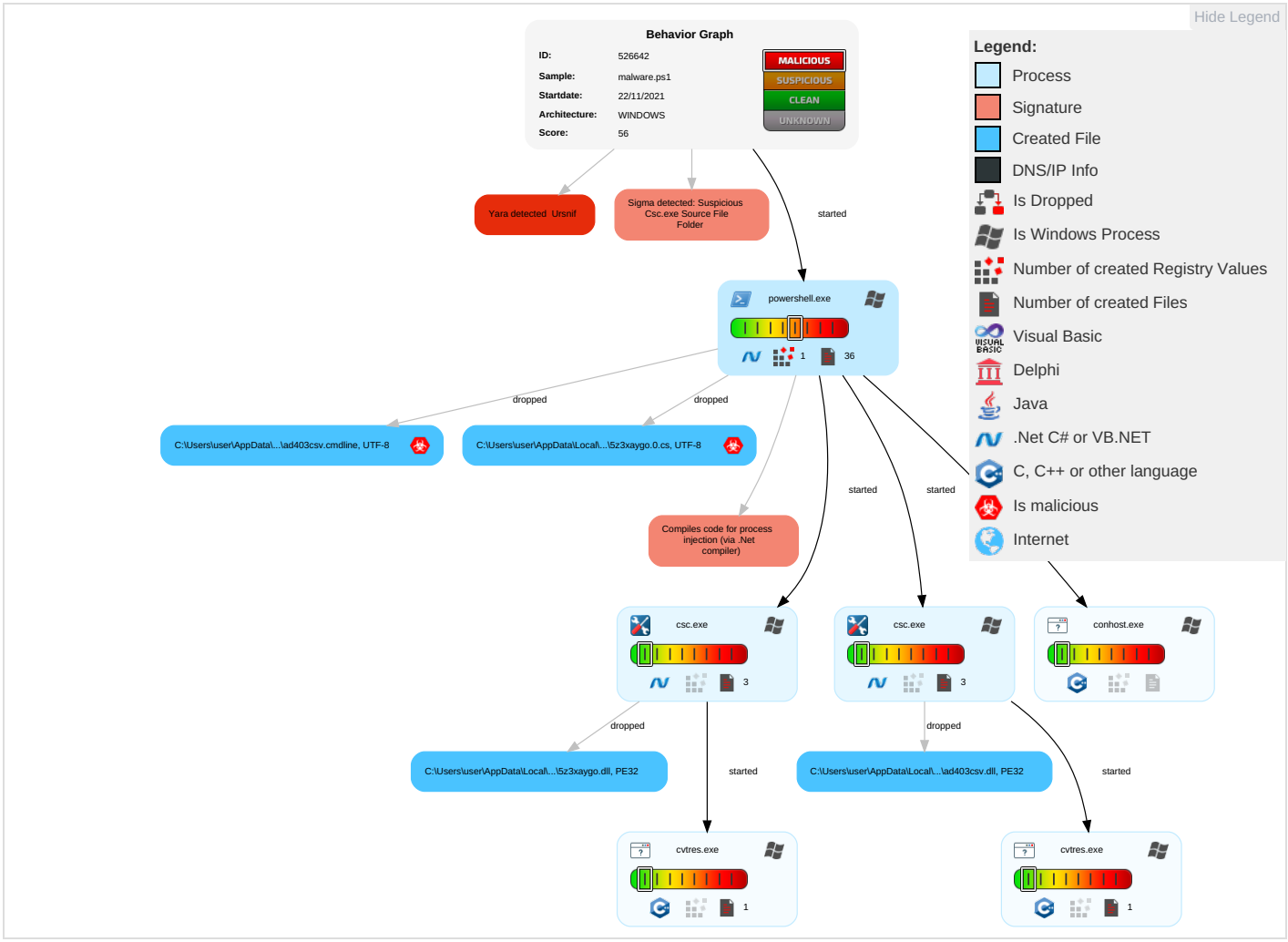
Yara detected Ursnif

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	Windows Management Instrumentation	Path Interception	Process Injection 1 1 1	Masquerading 1	OS Credential Dumping	Process Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 1	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 1	Security Account Manager	Application Window Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat

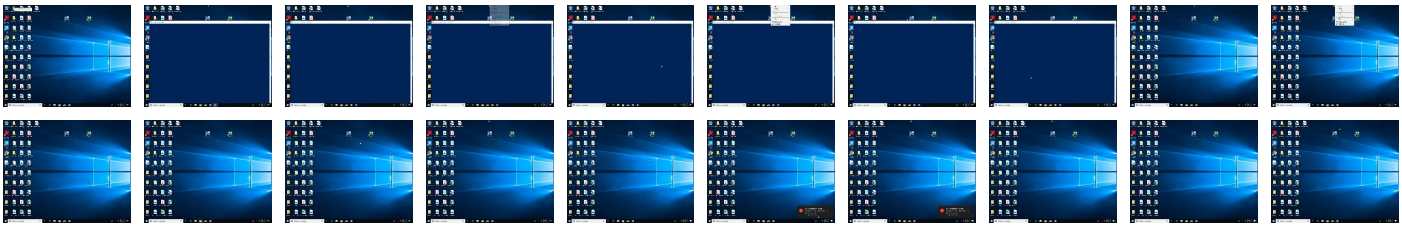
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://oneget.orgX	0%	URL Reputation	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://https://oneget.orgformat.ps1xmlagement.dll2040.missionsand	0%	URL Reputation	safe	
http://https://oneget.org	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	526642
Start date:	22.11.2021
Start time:	20:41:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	malware.ps1
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:	28
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:	mal56.troj.evad.winPS1@10/19@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .ps1
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:42:48	API Interceptor	36x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	9432
Entropy (8bit):	4.918232018284106
Encrypted:	false
SSDEEP:	192:Nxoe5FpOMxoe5Pib4GVsm5emdygkjDt4iWN3yBGHh9smidcU6CGdcU6CS9smDpOh:bfib4Glkjh4iUxs14fib41
MD5:	F6775EDC5EE3B8EEDBF8310BD48C709D
SHA1:	51DBC51183BFBFE57F24E9AD63840E60D2E64842
SHA-256:	B5D6E4B1EF4F3E734E47F87E8226814AE7D574F4E458CCE4E21D637588F45B28
SHA-512:	EDCED69415369C7EBA17D72EC1691FE44F5C5DCF7565EAE1A22112E631FFBBCE72B830BBF0D91E70484BC7F0E4D59870777B07E86126438E78E15A7337D97BE6
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\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-DscRe source.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.... ....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDrive eItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NllluIb/lj:NllUb/l

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82941 3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\5z3xaygo\5z3xaygo.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	426
Entropy (8bit):	5.033139906052158
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJ3eIVMRSRa+eNMjSSRrtXuSRHq1zyaRMseeBVtEvwy:V/DTLDfuRXl9eg5rtVuzyleBKwy
MD5:	4D67B4EE9B0124EA3067CCCC7F44B80F
SHA1:	2FE1AFC564476F305A0E2D3F57FC067E3C08E594
SHA-256:	5F263A0DD8E22A4DE11BC5870D10AE9B8D6DFD3CF5CBE915ACE34F747E88C225
SHA-512:	6CA77C9F0D56A036715ABD769E54236F66E7F8FE25CA1B3979DA81976E25AE7B655781A4D141B5C87CFBD5195BB2DC71D1B9D15B875C244FE8EEBDA72624E1 7
Malicious:	**true**
Reputation:	low
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class fvjclmvowuq. {. [DllImport("kernel32")].public static extern IntPtr GetCurren tProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint ylhvvsufcha,uint rxyvxpo);.[DllImport("kernel32")].public static extern IntPtr VirtualAllocEx(IntPtr jhx, IntPtr fapfrwulaod,uint ucg,uint nhatlxexrfg,uint mbnnbncpkga);.. }..}.

C:\Users\user\AppData\Local\Temp\5z3xaygo\5z3xaygo.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	375
Entropy (8bit):	5.22678826498313
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723f0zxs7+AEszIN723fx:p37Lvkmb6K2asWZETaJ
MD5:	20B52BC8853F5D2BE49229A716754FEB
SHA1:	BDA79B5386D394C279767E15F17834CD651F743F
SHA-256:	49AA10C97AFD75C3814B6EA4317F0CE442C9F324106137FA42F7E2086211DEA7
SHA-512:	64B40A3A2E6E4BEAAFAEEFB4A3ACBE3788E1A5887DFEB0AF1875F1BE10DF7AEFB652A0A4D069FAF1EF25336BBC9E4358BF53A3046CF77B64A2A8449672A13 17B
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\Sys tem.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\5z3xaygo\5z3xaygo.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\5z3xaygo\5z3xaygo.0.cs"

C:\Users\user\AppData\Local\Temp\5z3xaygo\5z3xaygo.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.663517896017503
Encrypted:	false
SSDEEP:	24:etGS7M2Wreq8MTBo6EyX4oonTt9dWhdmWdFtkZfzmuWI+ycuZhNWhakSJGPNnq:6hYSMTBdlX4txDWjwJzmV1ulWha3J6q
MD5:	040180EB53B3B3A87643DE6679D5C04D
SHA1:	43E0D5256B21601EA3125AF53F476A60903ACA46
SHA-256:	16C6E413A2689D5BE2819042A810504F1B374D687EA79B9CE702454895C1137F
SHA-512:	79F9160F7E6A463A76D59EFDEB371EF9C14996FACF42498E5E2FAA6B05EB6A462BE6F41A7223EF60A14D83CF6E1A90A01C9E0E17A0FF2C8FE11AB646943B54D E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Oq.a.....!.....$... ...@..... ....@.....#..K....@.....`..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....$.....H.....X ..x.....(....*BSJB.....v4.0.30319.....l...P...#~.....P...#Strings.....#US..... ....#GUID...$...T...#Blob.....G.....%3.....7.0.....3.....#..... >..... P..... X.....P .....g.....m.....y..... .....g.!...g...!.g.&...g.....+.....4.F.....>.....P.....X.....

C:\Users\user\AppData\Local\Temp\5z3xaygo\5z3xaygo.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	878
Entropy (8bit):	5.3116865530466635
Encrypted:	false
SSDEEP:	24:KOuId3ka6K2adETaMKaM5DqBVKVrdFAMBJTH:ykka6CdE+MKxDcVKdBJj
MD5:	1580E6380AFE0D9DB61AA40C17A4530C
SHA1:	B10E77441799C04CF6CDD40A5802D75AD1D20F60
SHA-256:	B48258C4934220E0F779DF09AB4C4BBE5A96A583DAEBEE584352E48FD5431F0E
SHA-512:	1698DC0B7F1ACD641F6195ECB4B274F12B8A78E7A35569670495E0D2A6C455F6713DD9E6E1C5CA981E4A0B000BF290B30F558F6287F490B501CB4E064BC6C0C
Malicious:	false
Preview:	.C:\Users\user\Desktop> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\5z3xaygo\5z3xaygo.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\5z3xaygo\5z3xaygo.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\5z3xaygo\CSC84083F42CE6043C2AA7FFF454285CD95.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.114139857608812
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryYhak7YnqqJGPN5Dlq5J:+RI+ycuZhNWhakSJGPNnqX
MD5:	7FA0E1F63221C155E408DA71E83F6E6E
SHA1:	EC2D46E04B242574CD7D0D336A60B7CAF513730C
SHA-256:	A3AA7763BAD7A2910E682C2D32FBF77484CB6F9321097863B5AB6A6792D72BEA
SHA-512:	9558F1EC86ADED45B7529420F487E01FCBC8451AA501E7B02D7F17513D431C09F66D54B1F8A663992A3869B9AA12EAB4E1CFD2B0AD216D8148761D97FE622B4
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...5.z.3.x.a.y.g.o...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...5.z.3.x.a.y.g.o...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\RESD522.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x496, 9 symbols
Category:	dropped
Size (bytes):	1340
Entropy (8bit):	3.989892279138545
Encrypted:	false
SSDEEP:	24:HAK9ocaLGPjSSV+ytltbaHKhKKjmNII+ycuZhNkakSgPNnq9ed:KZLGPlbWAKMmu1ulka34q9+
MD5:	9B071EA6DBE78A67C2B1B88E91969853
SHA1:	A2DF5B27880F79FC0E0D81DB6A1FD1FF6A3E7F0B
SHA-256:	40303BB6F889DED464556E92DBE4CAA0C47148526076B316A64298A64C16C632
SHA-512:	B56AFD785743CC0BD3151FD53A3E1344CC245DEA056CC05EB98745756BD06693A98D38687F4E0C30F362D3B7774BB156FA2F9BB8B6AF57806EA8A822A2D6293
Malicious:	false
Preview:	L...Lq.a.....debug$S.....X.....@..B.rsrc$01.....X.....<.....@..@.rsrc$02.....P...F.....@..@.....V....c:\Users\user\AppData\Local\Temp\ad403csv\CSCD6795C79BDE3450B9F7CAA8771DF83B.TMP.....J/q.FJ.v..O.....7.....C:\Users\user\AppData\Local\Temp\RESD522.tmp.-.<.....'...Microsoft (R) CVTRES.a.=..cwd.C:\Users\user\Desktop.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...a.d.4.0.3.c.s.v...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....

C:\Users\user\AppData\Local\Temp\RESE4F1.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x496, 9 symbols
Category:	dropped
Size (bytes):	1340
Entropy (8bit):	3.998448659194412
Encrypted:	false
SSDEEP:	24:H0K9oVaOIb5/tbaHNfhKKjmNII+ycuZhNWhakSJGPNnq9ed:+IOIb5ct5KMmu1ulWha3J6q9+
MD5:	9BA5F00321F9F1F189A527689E8261ED

C:\Users\user\AppData\Local\Temp\RESE4F1.tmp	
SHA1:	A0C97B6FFE2C98D6AE379242E735DD87259A6886
SHA-256:	8EF1A8E1CB900DC0391E9511AB5376BFBDAC5D190853F860CE0253942DEC7FBC
SHA-512:	AE775ED38B0793B39E6AAFAD232D5BD8DA2BF134B655E1A9A54FC94766381D8C96710E3EB4712D2C191BBEA2B9A547FA4F524F2F629C1AC57D6CBA6866AD3D 8E
Malicious:	false
Preview:	L...Pq.a.....debug$S.....X.....@..B.rsrc$01.....X.....<.....@..@.rsrc$02.....P...F.....@..@.....W....c:\Users\user\AppData\Local\Temp\5z3x aygo\CSC84083F42CE6043C2AA7FFF454285CD95.TMP.....2!.U...q.?nn.....7.....C:\Users\user\AppData\Local\Temp\RESE4F1.tmp.-.<.....'...Micro soft (R) CVTRES.a.=..cwd.C:\Users\user\Desktop.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0..... H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n. f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...5.z.3.x.a.y.g.o...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i. g.h.t... ...D.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ebtshoty.hoc.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kc3e5p1v.f0a.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\ad403csv\CSCD6795C79BDE3450B9F7CAA8771DF83B.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0938605900949456
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5grySak7YnqqgPN5Dlq5J:+RI+ycuZhNkakSgPNnqX
MD5:	CC80E14A2F71D184464AB8761DDF4FAC
SHA1:	DDF8ED19C1ED06E84057996F31344ECD12B3974D
SHA-256:	45E82329E9000A6C5B1E88623E6D612BA83DCF206E9D6E348FE36AEEF4F61843
SHA-512:	E2BC82B91BFF5605453D77A37842D521D3B5AB3550D18CEDAC3514BF306A28ED5EC0E786015E7D2069657C192A54775406DE05EAE3D2C0E613673F496B69921I
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...a.d.4.0.3.c.s.v...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...a.d.4.0.3.c.s.v...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\ad403csv\ad403csv.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text

C:\Users\user\AppData\Local\Temp\ad403csv\ad403csv.0.cs	
Category:	dropped
Size (bytes):	414
Entropy (8bit):	5.012387590489786
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJc0H/VMRSR7a1gPc9OopxkSRa+rVSSRnA/fFOlN218zPQy:V/DTLDfuPH/ly/xv9rV5nA/NwSQQy
MD5:	E458C9B10EE5485711E8601EC2A9F7E7
SHA1:	52EBD94DA80BD5538C113C1A73BA0F773B3207F4
SHA-256:	10D6C8D84A31080F063B2FF734D3EC20DA046B698298723676C722C80D932683
SHA-512:	98F83BF02C6E41CDB284BC764B9F31231BA7936A086679333D8AA8A459448BCAE8A77765E3709EBB493FF274BF55F01282FB0EDA20391FC943E4BC0F184CF0E9
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class cnjja. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(IntPtr ljgjre,IntPtr eayjlqvhl,IntPtr sykorjnxna);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint hrlef,uint rrugydrmoih,IntPtr lsfhdtddyu);.. }..}.

C:\Users\user\AppData\Local\Temp\ad403csv\ad403csv.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	375
Entropy (8bit):	5.20961215785773
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fwWGdVzxs7+AEszIN723fwWGdQ:p37Lvkmb6K2aoWGdVWZETaoWGdQ
MD5:	134C2CEB0343B252C5A6ACB391EE310F
SHA1:	2380D4F3D56DAF0519BC83DCE794EB80BA4F060C
SHA-256:	B84F7591CA6C20051EDE5A22E96FC466DC72EB60612311F51EF1E42F7742E698
SHA-512:	1E3AE6C8E01E200FBB0D15DE0FAE21272E1E61848412E6D6244A4F1187CF5681EA90C2ADE6BBF241F297150E6F2D2113E8C841DF037DA1B854B56339F09BDB0
Malicious:	**true**
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\ad403csv\ad403csv.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\ad403csv\ad403csv.0.cs"

C:\Users\user\AppData\Local\Temp\ad403csv\ad403csv.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.628500986342098
Encrypted:	false
SSDEEP:	24:etGSIE8+mUE7R85lwCk3tQJ3pMa3864OFtkZfkVXDZ0WI+ycuZhNkakSgPNnq:69XE7S5lwh8jwJkVzZX1ulka34q
MD5:	A5A9F6F654FDF8623844B9A55444D3D8
SHA1:	AB6A5D3C9DE80729A5BCC54D1270D7C790CC150B
SHA-256:	2ABE984525B9E6A49B167534359D836B38CF9CBC1678144B49EA29B36554C8AB
SHA-512:	FEFBE43B7B630925354F12E41FEF11707F710CD8358E9C5610EAEE49767CF4B81F97067B57EB73CE3C29CFB6BBAE5B4D6C4920DD0CDC1A2C2B72FE04DFF9B354
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Kq.a.....!.....$... ...@..... ....@.....#..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....#.....H.....X ..d.....(....*BSJB.....v4.0.30319.....l...H...#~.....D...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....1.*.....(..... 8..... E..... X.....P .....c.....i....p.....z..... .....c. ...c...!.c.%...c.....*....3.;....8.....E.....X.....

C:\Users\user\AppData\Local\Temp\ad403csv\ad403csv.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	878
Entropy (8bit):	5.295832447682282
Encrypted:	false
SSDEEP:	24:KOuId3ka6K2aLGd6ETaLGdFKaM5DqBVKVrdFAMBJTH:ykka6CLGd6E+LGdFKxDcVKdBJj
MD5:	04A6796E30D4CF118EF2A40868C0CAC6
SHA1:	3714D88B8DBD53C668A4BFB19DB32DBB40FC2035
SHA-256:	08474F17337E78C616287D6519A9739183AD1C2A67624BE83017360E2209A3CC
SHA-512:	F1A12F65C7EE27B1422420AEEDE04B3107BD8608508F4BE1C2B3F64DEEAD333C62C69E7D97099EC9F453738CC19563BBFAD0689B20731154F7355D9FFFDFF7EA
Malicious:	false

C:\Users\user\AppData\Local\Temp\ad403csv\ad403csv.out	
Preview:	.C:\Users\user\Desktop> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\ad403csv\ad403csv.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\ad403csv\ad403csv.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6208
Entropy (8bit):	3.734032670342883
Encrypted:	false
SSDEEP:	96:y5Blp8CRCCV9KP9ykvhkvCCtrPXCiH9DKCiH9D2:mBlp8CnOIrPXtDKtD2
MD5:	0FD1067A8CEC6BEAFBE4E519D889010A
SHA1:	A555400C12826531732A170FB6FDA7673EF3DF3E
SHA-256:	CC8333C623065D16BB9ADB17F0BACD2F62D219A0F33B25BF3C01044F88A9BDA6
SHA-512:	2B5E0962E50A4F597DBE0BD3D87E05205956E9B706B59D085B615CD97FB33039986DA1A3A38CED1A0D5C2ADC29DA2617011A9F5DF5523FCB642ACE20DA567DD6
Malicious:	false
Preview:	.....FL.....F."... ...'+k.!-...V...a..\.....:..DG..Yr?.D..U..k0.&...&.....d.!-...{s&>.....@.$.....t...CFSF..1.....N....AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....N..wSN%.....Y.....t..A.p.p.D.a.t.a...B.V.1.....N....Roaming.@.....N..wSN%.....Y.....D...R.o.a.m.i.n.g.....\.1.....>Q.z..MICROS~1..D.....N..wSN%.....Y....._..M.i.c.r.o.s.o.f.t.....V.1.....>Qc{..Windows.@.....N..wSN%.....Y.....8E..W.i.n.d.o.w.s.....1.....N....STARTM~1..n.....N..wSN%...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..wSN%.....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\X0LX71ESHNRJY9TJQYH1.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	6208
Entropy (8bit):	3.734032670342883
Encrypted:	false
SSDEEP:	96:y5Blp8CRCCV9KP9ykvhkvCCtrPXCiH9DKCiH9D2:mBlp8CnOIrPXtDKtD2
MD5:	0FD1067A8CEC6BEAFBE4E519D889010A
SHA1:	A555400C12826531732A170FB6FDA7673EF3DF3E
SHA-256:	CC8333C623065D16BB9ADB17F0BACD2F62D219A0F33B25BF3C01044F88A9BDA6
SHA-512:	2B5E0962E50A4F597DBE0BD3D87E05205956E9B706B59D085B615CD97FB33039986DA1A3A38CED1A0D5C2ADC29DA2617011A9F5DF5523FCB642ACE20DA567DD6
Malicious:	false
Preview:	.....FL.....F."... ...'+k.!-...V...a..\.....:..DG..Yr?.D..U..k0.&...&.....d.!-...{s&>.....@.$.....t...CFSF..1.....N....AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....N..wSN%.....Y.....t..A.p.p.D.a.t.a...B.V.1.....N....Roaming.@.....N..wSN%.....Y.....D...R.o.a.m.i.n.g.....\.1.....>Q.z..MICROS~1..D.....N..wSN%.....Y....._..M.i.c.r.o.s.o.f.t.....V.1.....>Qc{..Windows.@.....N..wSN%.....Y.....8E..W.i.n.d.o.w.s.....1.....N....STARTM~1..n.....N..wSN%...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..wSN%.....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\Documents\20211122\PowerShell_transcript.618321.JkieqDuu.20211122204245.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1037
Entropy (8bit):	5.070558386980283
Encrypted:	false
SSDEEP:	24:BxSA57vBVLCF+x2DOXUW6YPMWKHjeTKKjX4CIym1ZJX2d69nxSAZ0:BZhvTLCMoORfKqDYB1ZY6BZZ0
MD5:	C5BD87614F655077736504819BD69035
SHA1:	61E8733EFA129F755D33934873638E6395756BE2
SHA-256:	08DD3D47C2F0865DD6B6567290471241485A858A936B16B6E59CA462FA7DC405
SHA-512:	D258813EA78D76C6DDB93ACFE97B1D47E0B28A463D4B8BCB62645A71539448CFDAD139C85DFF5BCDA71EAF8F1D92CB31CB87E2FBB81743C58557B8160A414C8
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211122204246..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 618321 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noLogo -ExecutionPolicy unrestricted -file C:\Users\user\Desktop\malware.ps1..Process ID: 5416..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: 20211122204247..**********..PS>CommandInvocation(malware.ps1): "malware.ps1"..**********..Command start time: 20211122204723..**********..PS>$global:?..True..**********..Windows PowerShell transcript end..End time: 202

Static File Info

General

File type:	Little-endian UTF-16 Unicode text, with very long lines, with no line terminators
Entropy (8bit):	2.53866846787868
TrID:	• Text - UTF-16 (LE) encoded (2002/1) 64.44% • MP3 audio (1001/1) 32.22% • Lumena CEL bitmap (63/63) 2.03% • Corel Photo Paint (41/41) 1.32%
File name:	malware.ps1
File size:	1508236
MD5:	b0b0657a4c375cffc126892c10b5acd6
SHA1:	580152e7c431a47fd0fe487b0171476de9b8e407
SHA256:	061eb7119db9995949b39369aed60c2c7617c82e580705206ce7b60de123aaa5
SHA512:	69936a043f995fbf282cbbecef741455917bf029bcaf74799e40477c64bb8b9051484fac495d4d19abaee7ef045972b9d0a25281a756d75622e4ed117c04bc04
SSDEEP:	3072:HX+LHMbCgauJGMRkcyMsSbpTNfQzuF5rk8dKG3Eqq7tFUtkqLVgd8dgHsehKEqf4:E
File Content Preview:	..$.b.f.m.d.p.u.w.=.".s.m.y.i.".;.f.u.n.c.t.i.o.n. .q.q.p.{.$.x.l.f.u.o.=.[.S.y.s.t.e.m...C.o.n.v.e.r.t.].::.F.r.o.m.B.a.s.e.6.4.S.t.r.i.n.g.(.$.a.r.g.s.[.0.].).;.[.S.y.s.t.e.m...T.e.x.t...E.n.c.o.d.i.n.g.].::.A.S.C.I.I...G.e.t.S.t.r.i.n.g.(.$.x.l.f.u.o

File Icon

Icon Hash:	72f2d6fef6f6dae4

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: powershell.exe PID: 5416 Parent PID: 5196

General

Start time:	20:42:43

Start date:	22/11/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noLogo -ExecutionPolicy unrestricted -file "C:\Users\user\Desktop\malware.ps1
Imagebase:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.393533159.0000014F2E95C000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

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: conhost.exe PID: 352 Parent PID: 5416

General

Start time:	20:42:43
Start date:	22/11/2021
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: csc.exe PID: 6196 Parent PID: 5416

General

Start time:	20:42:49
Start date:	22/11/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @" C:\Users\user\AppData\Local\Temp\ad403csv\ad403csv.cmdline
Imagebase:	0x7ff7be7f0000

File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cvtres.exe PID: 6324 Parent PID: 6196

General

Start time:	20:42:51
Start date:	22/11/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESD522.tmp" "c:\Users\user\AppData\Local\Temp\ad403csv\CSCD6795C79BDE3450B9F7CAA8771DF83B.TMP"
Imagebase:	0x7ff7545f0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: csc.exe PID: 6408 Parent PID: 5416

General

Start time:	20:42:54
Start date:	22/11/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\5z3xaygo\5z3xaygo.cmdline
Imagebase:	0x7ff7be7f0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cvtres.exe PID: 6424 Parent PID: 6408

General

Start time:	20:42:55
Start date:	22/11/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESE4F1.tmp" "c:\Users\user\AppData\Local\Temp\5z3xaygo\CSC84083F42CE6043C2AA7FFF454285CD95.TMP"
Imagebase:	0x7ff7545f0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Disassembly

Code Analysis