ID: 623387
Sample Name: file.exe
Cookbook: default.jbs
Time: 13:14:28
Date: 10/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

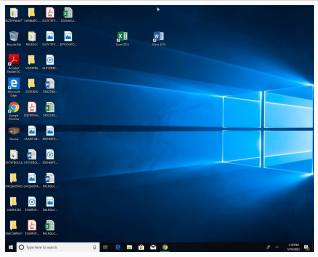
Windows Analysis Report

file.exe

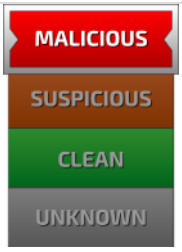
Overview

General Information

Sample Name:	file.exe
Analysis ID:	623387
MD5:	2beb53482de8f6..
SHA1:	0959ea9b1697d9.
SHA256:	7ac7845621113c..
Tags:	exe
Infos:	



Detection



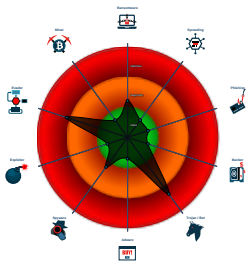
GuLoader

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Yara detected GuLoader
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains strange resources
- Drops PE files
- Contains functionality to shutdown /…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 6300 cmdline: "C:\Users\user\Desktop\file.exe" MD5: 2BEB53482DE8F6A713DEB6FA9F9E7267)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://msdvc.com/oluwa_RcQBQnZSyJ230.bin"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.784726043.00000000030B0000.00000040.00001000.00020000.00000000.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

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Networking

C2 URLs / IPs found in malware configuration

Data Obfuscation

Yara detected GuLoader

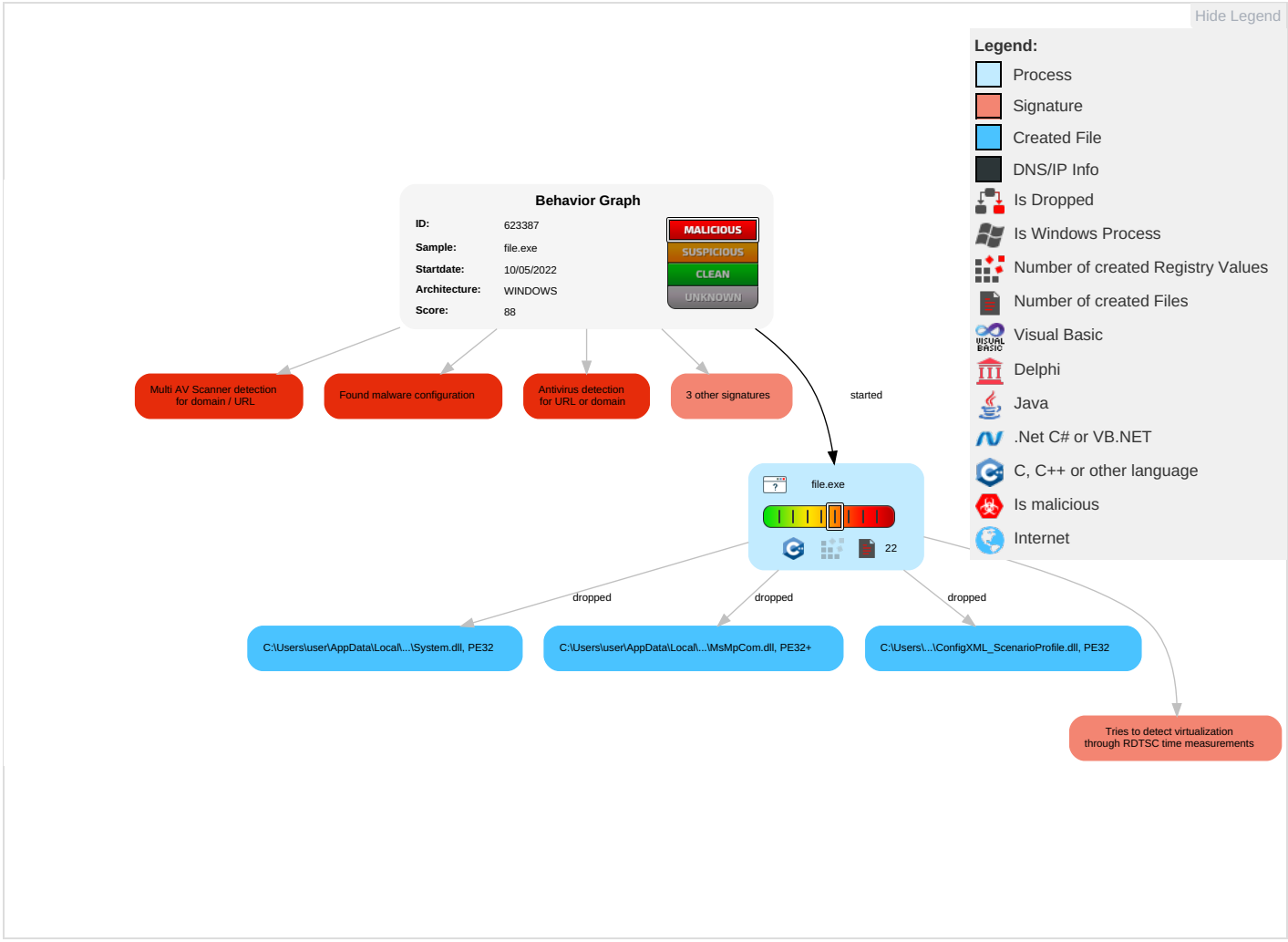
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

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 Native API	Path Interception	1 Access Token Manipulation	1 Access Token Manipulation	OS Credential Dumping	1 Security Software 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	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Obfuscated Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 3 System Information 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

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
file.exe	26%	Virustotal		Browse
file.exe	22%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\ConfigXML_ScenarioProfile.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\ConfigXML_ScenarioProfile.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MsMpCom.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\MsMpCom.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsaF229.tmp\System.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsaF229.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsaF229.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://msdvc.com/oluwa_RcQBQnZSyJ230.bin	5%	Virustotal		Browse
http://https://msdvc.com/oluwa_RcQBQnZSyJ230.bin	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://msdvc.com/oluwa_RcQBQnZSyJ230.bin	true	• 5%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	file.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	623387
Start date and time: 10/05/202213:14:28	2022-05-10 13:14:28 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
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:	mal88.troj.evad.winEXE@1/6@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.8% (good quality ratio 84.6%) • Quality average: 87.5% • Quality standard deviation: 21.4%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 52.242.101.226, 20.54.89.106, 20.223.24.244
- Excluded domains from analysis (whitelisted): fs.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

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\Aqua_3.bmp

Process:	C:\Users\user\Desktop\file.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, frames 3
Category:	dropped
Size (bytes):	5004
Entropy (8bit):	7.815894782719166
Encrypted:	false
SSDEEP:	96:BSTzRE92lvCfr4Y6hXqlvrfgAbJyLDLA4S+YrQslx:oXRnlKfrZ6h6lvncASiP
MD5:	12C11AD60C15E44F8297C052CFBAA434

SHA1:	3849A2C99770D1BB104AF27D34DCD95E8B4986A5
SHA-256:	71792E7507EE62E8EBC9BC1230947A8A4E2A5CAC57CD43DF1E379D91F5E3FDA2
SHA-512:	E91B30CFAFD4B651852D4F12E6A3BEF92A528C14C56FD195F6EA5EAF1D82308704BDD7373AA9DD63CE606BB25EAD7A33D29C8B068B843E0F1225177AA2F35E72
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d.....:Exif..MM.*.....Q.....Q.....aQ.....a.....C.....C.....n.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....(.....|2._.....&..?.i...x....o....xCB ..N..'.O..M..FW.o...C....+...,-.....~.....2.[....'..U.._.....]n..T.....".....>O.*.Z....j_...&|.....>.;q..B...L?.Mj^.bC..+k.. ..)..M(.....#.G..S....|7.oc:..o.....I.g.;]...../..I....U.>.`:._;...(....]...Y..=.....U'w..o.....%.3...

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

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	48360
Entropy (8bit):	5.965995469374706
Encrypted:	false
SSDEEP:	768:nd5SYvW5+CSHhidc/bBIa5bEd/w+D0OLzfmIHlsCdcAtpz3bi0M2X9DhH:d5xvFCwoMbGObqw20oBzbv
MD5:	81B2D0C87D9BE5FF6BBC1496BFEDFB4D
SHA1:	25D20CB862DC6690579513F1E9976FC03FC310E3
SHA-256:	B29472664E91D182B26F2BF2BD2171A4ADDB7132417C644DBD2CCE446A86923C
SHA-512:	F5769BF4981ED6E6DBE48D853A4951A800EB010350B3D2F79020CD9C9957EC193CF00BFD146FCB3CCAAE8C4EF2E5A25AA99C9314168EE6F432376CE410B74F7C
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a......" ..0.....V.... ....`.....O..... ..... ..H.....text...\.... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....8.....H.....xX..TZ.....0.....{....o.....{.....6.....{....(....&(.....o.....8...o....r...p....+A.....~....(.....(.....+..r...po ....-..{.....o ...r...p...X....i2..{....*.0.....{....o....{.....6.....{....(....&(.....o....&(!....o.....8...o"....8...o.....+B.....r...po....-7...8...%..=.o.....i.3.....{.....o ....X....i2..{....*..0.."..... ....s#..... .....(....&.o$...*...0../.....s%...&.r

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

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	88912
Entropy (8bit):	5.81677879181799
Encrypted:	false
SSDEEP:	1536:dRN1t8CahRmSzbibA1i552+B4KTeloLYlUY4GCmatsSR4P1:ft8oA1U2+mKTeCWJCmatsSmN
MD5:	B26386F33FAA0FC72A8077622ACC31B8
SHA1:	C9ECDB2123AB56818E999BB24B11A704462B290B
SHA-256:	C469ED974F4CC5DAA6EE7607927D2DE4500EAEAAEE66B267254FE6742F064BEB
SHA-512:	04E91D57F6DA63CB8196163EFD6D5726EE216DF1C649FFDB62E93450B92ED09CBC032DAC3CD62D8FB723AA40E08727784256AF54BC9847C095B6BCBCD0A45F2
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....H.....i..... ...Rich.....PE..d.../*.$....." .....e.....p.....`A.....D.....@.....0..4....:.P!..`..`.....T.....(..... .....text...?..... ..`.rdata...g.....h.....@..@.data.....@....pdata..4....0.....@..@.rsrc.....@..... .....@..@.reloc..`....`.....6.....@..B..... .....

C:\Users\user\AppData\Local\Temp\Ottawas.bmp

Process:	C:\Users\user\Desktop\file.exe
File Type:	PC bitmap, Windows 3.x format, 312 x 145 x 24
Category:	dropped
Size (bytes):	135774
Entropy (8bit):	6.91313068400418

Encrypted:	false
SSDEEP:	1536:GwfOK0U3CPBrtIu5/o0mrtd/Cl+DjS8Bn2C17WQ0SCoTsjwTxvXC0ntc9pKOIa58:LfObUqR2f7WQDTTxvXC0ntceOv7Wp
MD5:	3EEF656CBCA1AD683C0D205B8102AEEB
SHA1:	3601D8AEB56DA26777CFC229EDFB861A572CE78A
SHA-256:	A58CD5F1E7A2D07754798201CC1AC52E2BBC95AB2DA27E6F3556CCF50C719C2F
SHA-512:	F47676C91FD15160FB94C169FB9DC3361FE11F3E6C83AC2C6AFAF213DBAFD5875778C30A259E68CB491AE0EE99FA78EE6F68E60EC3094F4E09F8B83DD047D6CF
Malicious:	false
Reputation:	low
Preview:	BM^.....6...(...8.....(..... ....

C:\Users\user\AppData\Local\Temp\nsaF229.tmp\System.dll

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4.D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X.....text.... ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B..... ....

C:\Users\user\AppData\Local\Temp\touchpad-disabled-symbolic.svg

Process:	C:\Users\user\Desktop\file.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	786
Entropy (8bit):	5.0885849275192205
Encrypted:	false
SSDEEP:	12:t4C8glnVOtgVbYc7nz6F0EcWLjD8Gok9kXYJOhz4AeWrGDT2Kd3ztU7jcd/M:t4CjlQ2d7+5f4YLJw4AeWrGDT/nvd0
MD5:	B87E230E52E6179805CA646953B97596
SHA1:	DBE5466CA50A929245C5A09E003392B791A9C075
SHA-256:	D04DC1EDF72A3DE271177575A7F552FB3FFF450D9F1D2A6316D0FC953E78739E
SHA-512:	68572EFFC6200DD8F5395F659686F9C7F33DBF3864E445DC4FD8088A25784E256EAC10B75965B10E03B2B634BD4E0E78A09EBAAFAF5447CA3A00AB0B25DD36F7
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16">. <g fill="#2e3436">. <path d="M3.031 1a3 3 0 00-1.576.455l1.55 1.55c.01 0 .017-.005.026-.005h8.938C12.565 3 13 3.435 13 4.03V10h-3l1 1h2v.969c0 .298-.11.555-.293.738l1.402 1.402c.55-.549.891-1.306.891-2.14V4.03A3.038 3.038 0 0011.969 1zM.292.762C.11 3.149 0 3.577 0 4.032v7.937A3.038 3.038 0 003.031 15h8.938c.173 0 .34-.025.506-.053L10.527 13H8v-2h.527l-1-1H2V4.473zM2 11h5v2H3.031C2.435 13 2 12.565 2 11.969z" style="line-height:normal;-inkscape-font-specification:Sans;text-indent:0;text-align:start;text-decoration-line:none;text-transform:none;marker:none" color="#bebebe" font-weight="400" font-family="Sans" overflow="visible"/>. <path d="M1.531.469L.47 1.53l14 14 1.062-1.062z"/>. </g>.</svg>.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	5.79283030166378
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	file.exe
File size:	562640
MD5:	2beb53482de8f6a713deb6fa9f9e7267
SHA1:	0959ea9b1697d980da699f8375f91ca1df8e0f56
SHA256:	7ac7845621113c87e927eb2b582af6f1809e4866e4ee0f089dd1c6ab0042dd27
SHA512:	0484ee70dc3a77c36c4d6c846f3937cfbf116c4c6b7516e72660bbac8f6b3dcb01dac478c615f08fb180c27018e08ff023f11bdf46ae622b9b188956983c5d3a
SSDEEP:	12288:gNpIr3H1Fwz2KXE+7uAyZDSJSrF1v5/tLDD8W1qpwBaM8Af1:gNpIr3H1Fwz2KXE+7uAyZDcSrF1v5/t7
TLSH:	37C44B284B26D4E5CC8F2DB48C43B29F67922E50BAAD8253D53074E5EBFC366C7A5C11
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....f...*.....

File Icon

Icon Hash:	00f0f8e0ece07082

Static PE Info

General

Entrypoint:	0x4034f7
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9AE5 [Sat Sep 25 21:55:49 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	56a78d55f3f7af51443e58e0ce2fb5f6

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN="TRUISH Metaphysis BINDSAALER COUNTERPLEAD ", O=Countermarching, L=Gask, S=Scotland, C=GB
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 5/9/2022 4:04:21 PM 5/9/2023 4:04:21 PM
Subject Chain	• CN="TRUISH Metaphysis BINDSAALER COUNTERPLEAD ", O=Countermarching, L=Gask, S=Scotland, C=GB
Version:	3
Thumbprint MD5:	57E7BC9EC9D1474FF93F627A2D5F313A
Thumbprint SHA-1:	5C39BD33BBB4FB729C0C4634567294D7EDCB29F0
Thumbprint SHA-256:	C47A8A0C3B44E509CE176A357338FD2ADF724FE3389EA91AB0E6AB2804115F92
Serial:	07E4C4F966F11219

Entrypoint Preview

Instruction
push ebp
mov ebp, esp

Instruction
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007FD358730B0Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007FD358730ADAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A2D8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x48000	0x58810	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x88f48	0x688	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6515	0x6600	False	0.661534926471	data	6.43970794855	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.45	data	5.14577456407	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20338	0x600	False	0.499348958333	data	4.01369865045	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x1d000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x48000	0x58810	0x58a00	False	0.0791029398801	data	4.00672034737	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x48328	0x42028	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x8a350	0x10828	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x9ab78	0x25a8	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x9d120	0x10a8	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x9e1c8	0xea8	data	English	United States
RT_ICON	0x9f070	0x988	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x9f9f8	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x9fe60	0x100	data	English	United States
RT_DIALOG	0x9ff60	0x11c	data	English	United States
RT_DIALOG	0xa0080	0xc4	data	English	United States
RT_DIALOG	0xa0148	0x60	data	English	United States
RT_GROUP_ICON	0xa01a8	0x68	data	English	United States
RT_VERSION	0xa0210	0x2bc	data	English	United States
RT_MANIFEST	0xa04d0	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW

DLL	Import
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos

Description	Data
LegalCopyright	Ashland Inc.
FileVersion	18.4.12
CompanyName	Ceridian Corp.
LegalTrademarks	Enron Corp.
Comments	Cinergy Corp.
ProductName	InstallScript Setup Launcher
FileDescription	Hovnanian Enterprises Inc.
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: file.exe PID: 6300, Parent PID: 4180

General

Target ID:	0
Start time:	13:15:36
Start date:	10/05/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\file.exe"
Imagebase:	0x400000
File size:	562640 bytes
MD5 hash:	2BEB53482DE8F6A713DEB6FA9F9E7267
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.784726043.00000000030B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nssEAB6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406065	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
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	405AC1	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Ottawas.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\Aqua_3.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\ConfigXML_ScenarioProfile.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\MsMpCom.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\touchpad-disabled-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsaF229.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406065	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
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	405AC1	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AC1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsaF229.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405A81	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsaF229.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406023	CreateFileW
C:\Users\user\AppData\Local\Temp\nsaF229.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	3	406023	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nssEAB6.tmp	success or wait	1	40383F	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsaF229.tmp	success or wait	1	405C42	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Ottawas.bmp	0	18392	42 4d 5e 12 02 00 00 00 00 00 36 00 00 00 28 00 00 00 38 01 00 00 fd 00 00 00 01 00 18 00 00 00 00 00 28 12 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 12	BM^6(8(	success or wait	7	4060C3	WriteFile
C:\Users\user\AppData\Local\Temp\Aqua_3.bmp	0	5004	fd fd fd fd 00 10 4a 46 49 46 00 01 01 01 00 64 00 64 00 00 fd fd 00 3a 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 03 51 10 00 01 00 00 00 01 01 00 00 00 51 11 00 04 00 00 00 01 00 00 0f 61 51 12 00 04 00 00 00 01 00 00 0f 61 00 00 00 00 fd fd 00 43 00 02 01 01 01 01 01 02 01 01 01 02 02 02 02 02 04 03 02 02 02 02 05 04 04 03 04 06 05 06 06 06 05 06 06 06 07 09 08 06 07 09 07 06 06 08 0b 08 09 0a 0a 0a 0a 06 08 0b 0c 0b 0a 0c 09 0a 0a 0a fd fd 00 43 01 02 02 02 02 02 02 05 03 03 05 0a 07 06 07 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a fd fd 00 11 08 00 6e 00 6e 03 01 22 00 02 11 01 03 11 01 fd fd 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00	JFIFdd:ExifMM*QQaQaCCnn"	success or wait	1	4060C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ConfigXML_ScenarioProfile.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 13 0d 61 00 00 00 00 00 00 00 00 fd 00 22 20 0b 01 30 00 00 fd 00 00 00 06 00 00 00 00 00 00 56 fd 00 00 00 20 00 00 00 fd 00 00 00 00 00 10 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 01 00 00 02 00 00 fd fd 01 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELa" 0V `	success or wait	3	4060C3	WriteFile
C:\Users\user\AppData\Local\Temp\MsMpCom.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 48 fd fd fd 1b fd fd fd 1b fd fd fd 1b fd 05 1b fd fd fd 1b fd fd fd 1a fd fd fd 1b fd fd fd 1a fd fd fd 1b fd fd fd 1b fd fd fd 1b fd fd fd 1a fd fd fd 1b fd fd fd 1a fd fd fd 1b fd fd fd 1a fd fd fd 1b fd fd fd 1a fd fd fd 1b fd fd 69 1b fd fd fd 1b fd fd fd 1a fd fd fd 1b 52 69 63 68 fd fd fd 1b 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 2f 2a fd 24 00 00 00	MZ@!L!This program cannot be run in DOS mode.$HiRichPEd/*$	success or wait	5	4060C3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\touchpad-disabled-symbolic.svg	0	786	3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 3e 0a 20 20 20 20 3c 67 20 66 69 6c 6c 3d 22 23 32 65 33 34 33 36 22 3e 0a 20 20 20 20 20 20 20 20 3c 70 61 74 68 20 64 3d 22 4d 33 2e 30 33 31 20 31 61 33 20 33 20 30 20 30 30 2d 31 2e 35 37 36 2e 34 35 35 6c 31 2e 35 35 20 31 2e 35 35 63 2e 30 31 20 30 20 2e 30 31 37 2d 2e 30 30 35 2e 30 32 36 2d 2e 30 30 35 68 38 2e 39 33 38 43 31 32 2e 35 36 35 20 33 20 31 33 20 33 2e 34 33 35 20 31 33 20 34 2e 30 33 56 31 30 68 2d 33 6c 31 20 31 68 32 76 2e 39 36 39 63 30 20 2e 32 39 38 2d 2e 31 31 2e 35 35 35 2d 2e 32 39 33 2e 37 33 38 6c 31 2e 34 30 32 20 31 2e 34 30 32 63 2e 35 35	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"> <g fill="#2e3436"> <path d="M3.031 1a3 3 0 00-1.576.455l1.55 1.55c.01 0 .017-.005.026-.005h8.938C12.565 3 13 3.435 13 4.03V10h-3l1 1h2v.969c0 .298-.11.555-.293.738l1.402 1.402c.55	success or wait	1	4060C3	WriteFile
C:\Users\user\AppData\Local\Temp\nsaF229.tmp\System.dll	0	12288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	4060C3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\file.exe	unknown	512	success or wait	782	406094	ReadFile
C:\Users\user\Desktop\file.exe	unknown	4	success or wait	2	406094	ReadFile
C:\Users\user\Desktop\file.exe	unknown	4	success or wait	18	406094	ReadFile
C:\Users\user\Desktop\file.exe	unknown	4	success or wait	2	406094	ReadFile

Disassembly

No disassembly