ID: 632155
Sample Name: 72EED30398363-0983BNDJ0398763536.exe
Cookbook: default.jbs
Time: 11:35:56
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

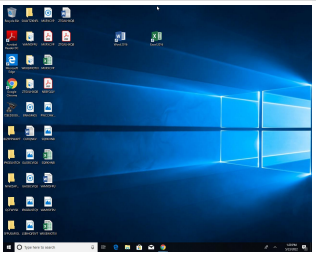
Windows Analysis Report

72EED30398363-0983BNDJ0398763536.exe

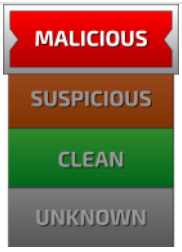
Overview

General Information

Sample Name:	72EED30398363-0983BNDJ0398763536.exe
Analysis ID:	632155
MD5:	511ad0297cd3e2..
SHA1:	aa466a3c5fb1a4..
SHA256:	c527fc06df0bca1..
Infos:	



Detection



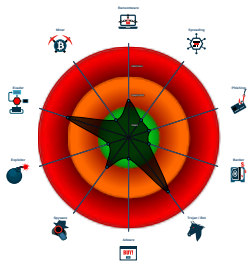
GuLoader

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- Uses 32bit PE files
- PE file does not import any functions
- Sample file is different than original …
- PE file contains strange resources
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- 72EED30398363-0983BNDJ0398763536.exe (PID: 5204 cmdline: "C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe" MD5: 511AD0297CD3E268E8D0C53C1207DC95)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.769168280.0000000003060000.00000040.00001000.00020000.00000000.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

Multi AV Scanner detection for submitted file

Data Obfuscation

Yara detected GuLoader

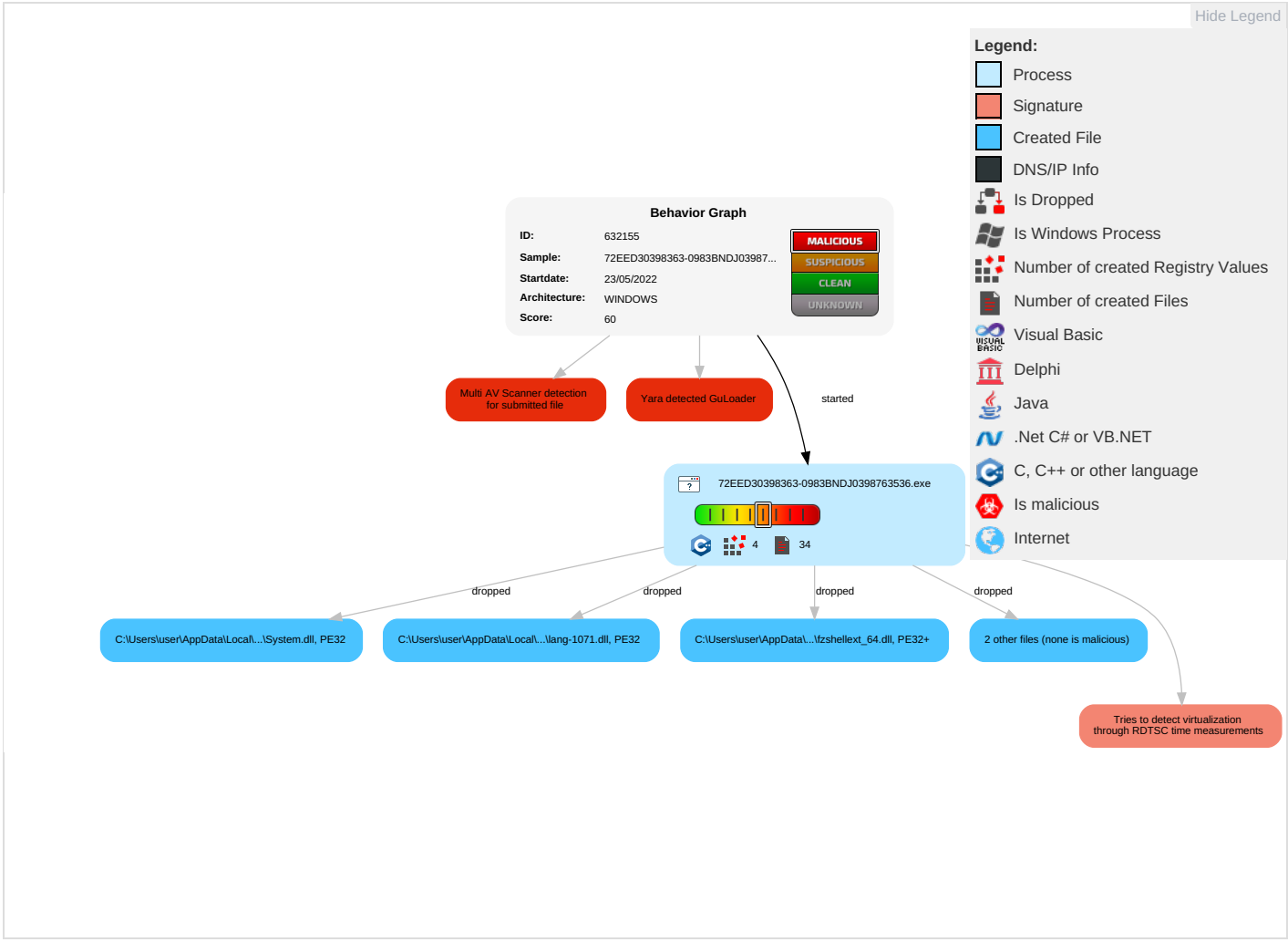
Malware Analysis System Evasion

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	1 Windows Service	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	1 Windows Service	1 Obfuscated Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	Junk Data	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

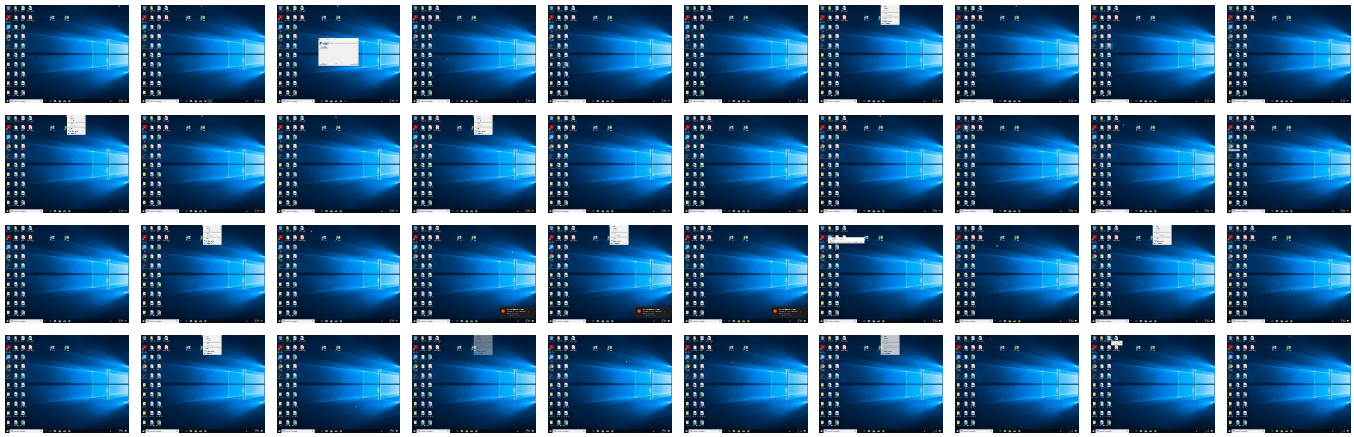
Behavior Graph



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
72EED30398363-0983BNDJ0398763536.exe	10%	Virustotal		Browse
72EED30398363-0983BNDJ0398763536.exe	5%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\MapiProxy.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\MapiProxy.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MapiProxy.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\Microsoft.Practices.ObjectBuilder2.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\Microsoft.Practices.ObjectBuilder2.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\fzshellext_64.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\fzshellext_64.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\fzshellext_64.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\lang-1071.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\lang-1071.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\lang-1071.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsw5376.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsw5376.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://www.avast.com0/	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://https://mozilla.org0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	72EED30398363-0983BNDJ0398763536.exe, 00000000.00000002.765958699.000000000278D000.00000004.00000800.00020000.00000000.sdmp, fzshellext_64.dll.0.dr	false	• URL Reputation: safe	unknown
http://www.avast.com0/	72EED30398363-0983BNDJ0398763536.exe, 00000000.00000002.765958699.000000000278D000.00000004.00000800.00020000.00000000.sdmp, 72EED30398363-0983BNDJ0398763536.exe, 00000000.00000002.762548137.000000000040A000.00000004.00000001.01000000.00000003.sdmp, lang-1071.dll.0.dr	false	• URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	72EED30398363-0983BNDJ0398763536.exe	false		high
http://ocsp.sectigo.com0	72EED30398363-0983BNDJ0398763536.exe, 00000000.00000002.765958699.000000000278D000.00000004.00000800.00020000.00000000.sdmp, fzshellext_64.dll.0.dr	false	• URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	72EED30398363-0983BNDJ0398763536.exe, 00000000.00000002.765958699.000000000278D000.00000004.00000800.00020000.00000000.sdmp, fzshellext_64.dll.0.dr	false	• URL Reputation: safe	unknown
http://https://mozilla.org0	72EED30398363-0983BNDJ0398763536.exe, 00000000.00000002.765958699.000000000278D000.00000004.00000800.00020000.00000000.sdmp, MapiProxy.dll.0.dr	false	• URL Reputation: safe	unknown
http://https://sectigo.com/CPS0C	72EED30398363-0983BNDJ0398763536.exe, 00000000.00000002.765958699.000000000278D000.00000004.00000800.00020000.00000000.sdmp, fzshellext_64.dll.0.dr	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:	632155

Start date and time: 23/05/202211:35:56	2022-05-23 11:35:56 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	72EED30398363-0983BNDJ0398763536.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.troj.evad.winEXE@1/14@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.8% (good quality ratio 61.6%) • Quality average: 88.9% • Quality standard deviation: 21%
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, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, www.bing.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, time.windows.com, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
11:37:05	API Interceptor	1x Sleep call for process: 72EED30398363-0983BNDJ0398763536.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\ARMOURY CRATE Message.VisualElementsManifest.xml

Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.284749695608875
Encrypted:	false
SSDEEP:	3:ejHERMQnFkViJS4RKbuviyiboBz5/Wo0WcL0yEyQEmkQV+Y7aMAUKl+HJDuMBXFQ:ejHyaVic4subiWzFWo1DhkQwY7hAUKms
MD5:	A1D0F1E580E02348560D8D7CB2A5A773
SHA1:	62A3B544C463CD164077BF00CFDDE45A92C8CDFA
SHA-256:	9E99E7F8983E7AFA447808263F0D539092DDCC9BD2D08DEC3955456DE3D82F0B
SHA-512:	69962F2E8201089F25EEC027443AC20DDB7F512ECAF65CC8964F68710FBD8CED2789EA946E30E3EB7ABA8FDD3A9B90842A6861D3F14F8EA96F9BE9D556EAAE9D
Malicious:	false
Reputation:	low
Preview:	<Application xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">..<VisualElements...BackgroundColor="black"...ShowNameOnSquare150x150Logo="on"...ForegroundText="light"/>..</Application>

C:\Users\user\AppData\Local\Temp\Airplane_14.bmp

Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.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):	9184
Entropy (8bit):	7.883950548629578
Encrypted:	false
SSDEEP:	192:oXRe/9ug6TLD7hE6T18DBHuJMlvNGi7aWCndwcKMwVof4aBLodMI:KRe/UfD1E658DFucGi2tdEILodMI
MD5:	8DF53262DD7366ACC7CA948D11197771
SHA1:	3902822B1E93424F83731C8FE0FCC0C6B25E5CA7
SHA-256:	744D858D6C6A7B6E771A5B2D09A0DE81DF56BA28DCC15BA803871A97513C345C
SHA-512:	0BD2C0D7CC5A82EABABA1A9820C4D1905ABD00416B20C995AD26869B3A38246A9808BA879FA90435C559AC574793FB4E79785C6E023CE0A242DD90BA4FE29578
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d.....:Exif..MM.*.....Q.....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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....Q..?`.....?.g.m...^$....K.K\./.t..F...q#2M<.#.c.U..P0F.....1....Z.]....y..kxs...*=.&A.-.....].Z.3...?...6..q..._....z....Q>...].V....E.*.../Pq...F....:u#h7...8.T.NW..' ...O.%...&..7.....*.....~...'.~.bo.%G..2.}...8~..S.5...C.r.....<.U..w....o..=.nW.9#.....H....u...om....L....1U.y....<..

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

Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20920
Entropy (8bit):	6.270129738401503
Encrypted:	false
SSDEEP:	384:35kgh9IGJLE8rIYcnuYPBkvDG/Ghu4aX9lw:pkM9IG9EWIYyusqDGehuDXvw

MD5:	22ACDFF46574615C4EBF05E223A15899
SHA1:	45A3ACFE2D98A8AED780F0A323DA8B2BE366D2B6
SHA-256:	3089869E2C5691A16E1CF677BAB0A9148B688FBC6B69BB9AF949DD5AC009B063
SHA-512:	9D689705A5737F557B8FCC84DB49E1B36EE8E527D8150DA5E8766BA50298CA0791224E90C7DADF9D930EFD4D0E113E387496F03F672C865E6A5785D12C7859B
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....#b.....''!.....`.....t....@A.....'.....(..d...`..x.....2.....p.....&.....H&.....).....text...~..... ..`.rdata..D.... .....@..@.data..... 0.....$.....@....00cfg.....@.....&.....@..@.orpc...<....P.....(..... ..`.rsrc...x....`.....*.....@..@.reloc.....p.....0.....@..B..... ....

C:\Users\user\AppData\Local\Temp\Microsoft.Practices.ObjectBuilder2.dll

Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	63104
Entropy (8bit):	5.896544515767483
Encrypted:	false
SSDEEP:	1536:gmnKEGwDMO8sr1HmWaCoTcmfN/YYFH0CUYyFB6yhvfQvDYXX:LnKEGMDAcmfUF3Q7YXX
MD5:	BA1836B308145CB718436BDB13AEEE22
SHA1:	DB1058FB7CF495F41DE09EE7B851C6689498AB71
SHA-256:	CCD5DE1DB4C4BAA22EAC952A83CEC144A1038556959255E5EB202E0C8C1C4C66
SHA-512:	3F06969280877BE4828A5070BB43461AE63B9110A6192BAD3A9C9390A12AF47E44024D06A7E5243A5FD5F659910199F8D5157055C15C605EFA8287E9075D1AFF
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....$.....PE..d...G..S....." ....@.... ....}.. ..@...@.....@..... .....@.....@..... ..H.....text...{.... ....`.rsrc...@..... .....@..@.reloc..... .....@..BH.....j..<.....`.....0..-.....oC...(.....(....%-.&..(.....,...(....*.*....0..m.....sT.....o.....+O..... (.....8...o.....o.....o@....o...+.o@....oC....(d.....oE.....X.....i2..*J.....(.....o....*.0..s.....o....(...+~ ...-....!...s".... ...~ ...o#...o$.....i..E.....+..*...*(%...(.....o&.....(' ...s(...z..0..w.....o.....s)...(...+..i..E.....+..*...*...o.....i....o.....i.3/

C:\Users\user\AppData\Local\Temp\Sports-Wallpapers-1.jpg

Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x786, frames 3
Category:	dropped
Size (bytes):	782753
Entropy (8bit):	7.972739118836816
Encrypted:	false
SSDEEP:	12288:1xE6g9kiViGNq+W6nQNIDO0tVGb34eaR6fUnMlkTFztQywzV0jyB4Dl9l+qfkwPN:7E6G3VibpHIdebodR6jlKFtQVUv+iP8S
MD5:	E269DECCAC13CF01A0377872E79BC676
SHA1:	54D196FDE9529310F9E5A3EBA6548DAB4F179542
SHA-256:	255874E0A6A5CA862CBAE5C783D582729B343C70C5697062D7F1E587F15F25EC
SHA-512:	08ADAD38BE3472CF8814C40F99D6DCFDA313C2FED765B872AA30C0995B027F2BEDABF75DB625F3C40F003A8EFC3F41169CBA4AF706EC637018DEEF02EC92F 6CC
Malicious:	false
Reputation:	low
Preview:	.....JFIF.....`.`.....XICC_PROFILE.....HLino....mntrRGB XYZ .....1..acspMSFT....IEC sRGB.....-HP .....cprt...P...3desc.....lwtpt.. .....bkpt.....rXYZ.....gXYZ...,....bXYZ...@....dmnd...T...pdmdd.....vued...L....view.....$lumi.....meas.....$tech...0....rTRC...<....gTRC...<....bTRC...<....text....Copyrigh t (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1.....XYZ .....Q.....XYZ .....XYZ .. ....o...8.....XYZ .....b.....XYZ .....$.....desc.....IEC http://www.iec.ch.....IEC http://www.iec.ch.....desc.....IEC 61966-2.1 Default RGB colour space - sRGB.....IEC 61966-2.1 Default RGB colour space - sRGB.....desc.....,Reference Viewing Condition in IEC61966-2.1.....,Reference V iewing Condition in IEC61966-2.1.....

C:\Users\user\AppData\Local\Temp\TREDIVER.Und

Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	data
Category:	dropped
Size (bytes):	96538

Entropy (8bit):	7.127885129617323
Encrypted:	false
SSDEEP:	1536:QLcub+0B+L4nRYjPjhDxPA0Z8sHmIYnlklScwN2hUrVMr01Rt:QXb+U5nRYjLl5A0RHInlpcN2Eo
MD5:	BE404281EAEDF107215373147BD63124
SHA1:	21677AF0A0E1C95E1F5444DB62858E022F7A625F
SHA-256:	676542C7435A8B1D2984027E2B10D47A3403179BA355D6BA2761D056754B4226
SHA-512:	678725B6869F362A85E0000EA7F5669145F1CFE20990CB78E20F3E0BE156FA3C8A315CEE257E765783C3FDCC44B152B944E5FC31F3BF8F7AF8C5363B97DE92B B
Malicious:	false
Reputation:	low
Preview:	...<X..0<:..6.....<.....&...<..$..-..n.B.....C<.<...}<]...<0<....F...<P...........<.<...<...N<.<...b.....<...`1.<:..`...<]<3...<...<.<...%.....<...<.<y....'<8<..D<....<l<........$.4../8n...<$<`.....<S<...4<...(<.<$.............X<8<O..)..l<h<@...<....<.<..........{....u.....<t<..!..@<.<....i<....<.<.........h...<n<O.....<!<...<...d<x<.............4~9n.~5V.....iv.....E..=b.m,...S.\...G. F[E..''..|...0C....d._....\..7.P<.....a.i4l...Z!U.....Z-.N..M.}r...''.2..#.....Y6.....z..GR..V..Q. ../.k..zz.V..+...u.....*.x.f.G..g=s.....%..... ...Ckw..... ?....~TMw....<]....:A.f..>.e[.+5..6.u4..X.....G''...J.....^.6.....6.....T..''..... .....J.....

C:\Users\user\AppData\Local\Temp\format-justify-center-symbolic.svg

Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	319
Entropy (8bit):	4.594821675408072
Encrypted:	false
SSDEEP:	6:TMVBd/6o8GUYl/n7S3mc4slLlNkRIhFYV4vtAlaRI1stAlaRIH32tAlBC:TMHdPnnl/nu3tlnTPvWlzyWlzH32WlM
MD5:	494915A7B4C3DFA64D1F4CD789C8CC97
SHA1:	5873C59C31EF784AAE90D8EE0EBCD5BB2FCFB673
SHA-256:	8E229CFBC1B7D593409310662867493B644FA07C68CA60F64018B1CDBC7FAC04
SHA-512:	11BD7CF250A2F45E0FB79906478B3B2AABC8032622A2ED898EDE6E5AB077FDF6ED55DFA1B9EE54BF8E36BB7EC7BD7E533D2F8143DA15E8F7DA9EB9360F4B2 82B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<svg height="16px" viewBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg">. <g fill="#2e3436">. <path d="m 3 2 h 10 v 2 h -10 z m 0 0"/>. <path d="m 1.003906 7 h 14 v 2 h -14 z m 0 0"/>. <path d="m 5 12 h 6 v 2 h -6 z m 0 0"/>. </g>.</svg>.

C:\Users\user\AppData\Local\Temp\fzshellext_64.dll

Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	28712
Entropy (8bit):	5.958396786343478
Encrypted:	false
SSDEEP:	384:Jw9Wl09pPemQKLJO8WwTB4NTRFRz2X9f512mG5dKlLnyrVU9XhGfZyhq:e9WlcGlgJWsZbH3DyiXmyh
MD5:	1438E9F76917193C424B15094683D2EB
SHA1:	85EED842A0F06CBBA53A08A231AF8CBE66BB89DB
SHA-256:	84FFF6EA83E615D85D6BE156A2443AC966A7172A2C5C50727B0D75AE99822EDD
SHA-512:	F8A522814B9277674BDC7B118FE9133CEC3BF521FBD617103565E8EBF5CEF11D66E1C84734000D7DB0441480BD5EEED6AB8D776319D80CE57DCAB46F5D77C4 4A
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....."...#."...H.....P.....g.....@^.. ..`... .....x.....`..T....L...($.....|.....R..(.....text....!.....".....`.P`.data...`....@.....&.....@. P..rdata.. ....P.....(.....@.`@.pdata..T....`.....0.....@.0@.xdata..0....p.....4.....@.0@.bss.....`..edata.....8.....@.0@.idata.. x.....:.....@.0..CRT....X.....B.....@.@..tls.....D.....@.@..rsrc.....F.....@.0..reloc..|.....J.....@.0B..... .....

C:\Users\user\AppData\Local\Temp\lang-1071.dll

Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	104272

Entropy (8bit):	4.543275874610095
Encrypted:	false
SSDEEP:	3072:yw4+Ma1g2FYhTaV2NTzgbevXKrmFqYyfZ:y43VqsTT
MD5:	DB49F13C9928754DEAEBBF869638897D
SHA1:	A97B054292DF83EC70697C740955E837B3573653
SHA-256:	B42A530B4DCACA8E43AD71A7E6383273DB29D3660AC0F84FE26AABEC69724EBE
SHA-512:	0CB79A2396A683B8B4CFE634B5CB99F17239CE828174A1B623183A3E1BBB458BD4B77121C019E00444923D97F53ECEC4011AAD86D624BCC6084E64AE7B220B9 0
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....$.....<...R...R...R.@...R.@.P...R.Rich..R.....PE..L....*j^..... .....!.....t.....@..... ...p.....v..P!.....rdata..p..... .....@..@.rsrc....p... ...r.....@..@.....*j^.....T.....rdata.....T....rdata$zzzdbg.... ..P....rsrc$01....P9...W...rsrc$02..... ....

C:\Users\user\AppData\Local\Temp\mail-reply-all-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	244
Entropy (8bit):	6.758520539988057
Encrypted:	false
SSDEEP:	6:6v/lhPys81g2WMTrmv2GxdaTKUWdXhcorhOZXd5bvn0LGp:6v/7c1ZWarYvDa+UWdxcor87bv0g
MD5:	4FD7AA500BD09F4AE3D4D0951D56B095
SHA1:	215730E32EE69DBA4A8CCF190D16903C51803C3C
SHA-256:	B34B352C04C4578B1130C979A3571DBF058BC939CDC45723E479BCE27D80B7A5
SHA-512:	B4EEA2408A0A717EE79DB3BD66DFDA455A67058CF707F5638DF786DADFFEBE0E9DFF508DA6ED235AE5AD73EE82656C1338590910850A046B66ECB82AEE19B 036
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...?jBA.....)...!<....y..a.T.H .....g.<X.....[|3.3...1.'..oe..(...V.....]~..U.4.....2.\..^....S.....<9.OL.c..K|s.S.Wy.1..|..U..j^i.{(.. ..J..5..E4.V.....2...t.....IEND.B`.

C:\Users\user\AppData\Local\Temp\media-playback-start-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	195
Entropy (8bit):	6.430880464743636
Encrypted:	false
SSDEEP:	6:6v/lhPysmh8PfdN0KGI78rYLxrXDvSIKyVirp:6v/7G2PX0Xh8xKIlk
MD5:	DA92549587296011343070 6C4C2EC1D7
SHA1:	4B32A4996BA978F85E59A6F680BD7284FA5CEF25
SHA-256:	6163611AC321BBD145F39CA05A7B55F38C54D22D9A5E0898DA72E6E1200FA26B
SHA-512:	3F9FAC6703682550CC259CD2A2EEEF47CAF2C87A851D08B89C4C0CB4D9829652B9851EB71F62D8B27CD079BDFCC2B683368D14A12A3D94C32290D8C80B71D 9
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....zIDAT8.....P.E...&.....e.....C$Rh.r.(.?O..m=...<qA...3NXg...]. .....p.&+.&.....o..)..F.h....x....>.K.i.Q..3.....a..(o:....IEND.B`.

C:\Users\user\AppData\Local\Temp\network-no-route-symbolic.svg

Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1260
Entropy (8bit):	4.838834785988535
Encrypted:	false
SSDEEP:	24:t4CpQOpbZmi4vxMgThS3UunhEXJaTAjpw4AeWrGMyWd3vCmLyxmhwLsBBL03PhXB:2yOxMgTihkWAjG4Ae3MZtOmh+4BLtYxH
MD5:	03A35EC7CB5A202A491FB84A5EACE46E
SHA1:	476405E7FAEE6B36C7F955CFA09FE304E50BD6D3

SHA-256:	C5154D6254D127A9DF95CAC18364FE23E124BC9D66A84B59CC269FA51CEC18B9
SHA-512:	7439E4020259B4850F4EC208B0EFB10611479DE4F80619D47DCD4E9F94DF1FCB1BBC2B416DC084D44D06E30ADF30A2A16B3E66C9D374FFBC7B49920EC6F91EC
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M10 1v1c0 .257.13.529.313.719L11.593 4H8.23a4.034 4.034 0 013.273 2h.123l-.074.078c.27.495.449 1.047.482 1.647l.002.029v.027c0 .265-.021.516-.052.762L15.406 5 11.75 1.281C11.552 1.091 11.31 1 11 1zM7 4c-.294-.004-.559.15-.746.371.416-.2.871-.321 1.348-.371zM4.068 7.406L.594 11l3.656 3.719c.198.19.44.281.75.281h1v-1c0-.257-.13-.529-.312-.719L4.406 12h1.971a1.723 1.723 0 01-.34-1.04 2.77 2.77 0 01.18-.96H4.375l.98-1.031H4.09l-.053-.944a3.717 3.717 0 01.031-.619z" style="line-height:normal;-inkscape-font-specification:Sans;text-indent:0;text-align:start;text-decoration-line:none;text-transform:none;marker:none" color="#000" font-weight="400" font-family="Sans" overflow="visible" opacity=".35"/><path d="M7.848 4.969c1.642-.092 3.096 1.17 3.188 2.812 0 1.402-.378 1.922-1.594 2.844-.191.144-.326.25-.375.313-.05.062-.031.033-.031.03.007.529-.472 1-1 1-.529 0-1.007-.471-1-1 0-.502.224-.943.468-1.25a3.82 3

C:\Users\user\AppData\Local\Temp\nsw5376.tmp\System.dll

Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
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: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
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\system-reboot-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	327
Entropy (8bit):	7.015504476308313
Encrypted:	false
SSDEEP:	6:6v/lhPyshpTgb5VYwsMgZx9dumoUd+g2n7dbfMdHegZQy2SxpqliJv/Ct5r1qt7p:6v/7Mb52YKdUTgZQlRv5m
MD5:	B23317C72FF4A53029CEBBA876561AE1
SHA1:	5127AF4C76241B78CF253AF98DF35594B0693B2D
SHA-256:	07488F4DCE56A1DE0ED909541581A63B0498663DDF532707BFD01D77224A1D31
SHA-512:	CE4E5C61EBB736688E437330B65192E4A53703128299B067569E5E56281284A8592FD8C0C88B1CE4052CFB8F2C2BD6A129074BAA649D06DBF7F314C4ADB3209
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...;J.A....j. ...{.x...}.{.=...x...(.... "..gpU.._..M;3+XPt.W5..j.i.K.....N.,...c.h..d..p.',..V...8.....@+.....1.....S.M.....2.....b;.."....#.....M.%.!..?..b}L..X..7U..F.....^.#l6...~.T^..\.....l..8..'V...M.T.3....Y.....OD.,.P....IEND.B`.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.738214112700285
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:	72EED30398363-0983BNDJ0398763536.exe
File size:	1141532
MD5:	511ad0297cd3e268e8d0c53c1207dc95
SHA1:	aa466a3c5fb1a4c3ae77835fc3d592e8f7a0679b

SHA256:	c527fc06df0bca1fe6ef47ff82e1a858af8b50877d97446c7898e5d1a80146a3
SHA512:	1667daacf36e47caf1a061fc9725a0692317def2b0c2c0017ebf5ca75046501dc107ec94a0ddd74ac11c7d9bbbe7c5cc16c163ba5aac5879ba6c8469ba079924
SSDEEP:	24576:kY8XnAQGPnlkfWFUK0jqyUEcq7mGLtxSdrHYZ8OI6LG5P4dNg:tHQGNYWFUJuyUA6tdTnO5i5wdu
TLSH:	85351261B336C40FD442E93D1B5FD3994AABAC502F69CDD63210AB8FAE346046F497B4
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.....h...*.....

File Icon

Icon Hash:	78f8a4d9f47eb95a

Static PE Info

General

Entrypoint:	0x403640
Entrypoint Section:	.text
Digitally signed:	false
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:	0x614F9B1F [Sat Sep 25 21:56:47 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:	61259b55b8912888e90f516ca08dc514

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
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], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
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 00007F6550CBC4BAh

Instruction
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 00007F6550CBC48Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], 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	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x74000	0x28488	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
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	0x6676	0x6800	False	0.656813401442	data	6.41745998719	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.14106681717	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.11058212765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x49000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x74000	0x28488	0x28600	False	0.342685758514	data	4.39207892807	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x74358	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x84b80	0x94a8	data	English	United States
RT_ICON	0x8e028	0x5488	data	English	United States
RT_ICON	0x934b0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 8454136, next used block 4294967167	English	United States
RT_ICON	0x976d8	0x25a8	data	English	United States
RT_ICON	0x99c80	0x10a8	data	English	United States
RT_ICON	0x9ad28	0x988	data	English	United States
RT_ICON	0x9b6b0	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x9bb18	0x100	data	English	United States
RT_DIALOG	0x9bc18	0x11c	data	English	United States
RT_DIALOG	0x9bd38	0xc4	data	English	United States
RT_DIALOG	0x9be00	0x60	data	English	United States
RT_GROUP_ICON	0x9be60	0x76	data	English	United States
RT_VERSION	0x9bed8	0x270	data	English	United States
RT_MANIFEST	0x9c148	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
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, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, 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	Copyright 2018 Google LLC

Description	Data
FileVersion	1.3.36
CompanyName	Google LLC
LegalTrademarks	
Comments	
ProductName	Google Update
FileDescription	Google Update Setup
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: 72EED30398363-0983BNDJ0398763536.exe PID: **5204**, Parent PID: **6060**

General

Target ID:	0
Start time:	11:37:01
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe"
Imagebase:	0x400000
File size:	1141532 bytes
MD5 hash:	511AD0297CD3E268E8D0C53C1207DC95
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: 00000000.00000002.769168280.0000000003060000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsa450C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsa450D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	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	2	405C22	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	2	405C22	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	2	405C22	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	2	405C22	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	2	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\TREDIVER.Und	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\ARMOURY CRATE Message.VisualElementsManifest.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\Airplane_14.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\MapiProxy.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\Microsoft.Practices.ObjectBuilder2.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\Sports-Wallpapers-1.jpg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\format-justify-center-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\fzshellext_64.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\lang-1071.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\mail-reply-all-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\media-playback-start-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\network-no-route-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\system-reboot-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\docoglossan	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\docoglossan\Clerkish	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsw5376.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	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	405C22	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	405C22	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	405C22	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	405C22	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	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsw5376.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	405BE2	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsw5376.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\nsw5376.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	5	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsa450C.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsw5376.tmp	success or wait	1	405DA3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	32768	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	406224	WriteFile
unknown	44223	21515	75 6e 6b 6e 6f 77 6e	unknown	success or wait	62	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\TREDIVER.Und	0	16384	fd fd fd 3c 58 fd fd 30 3c 3a fd fd 36 fd fd fd fd fd 3c fd fd fd fd fd fd 26 fd fd fd 3c 80 fd 24 fd fd 2d fd fd 6e fd 42 01 00 00 fd fd 43 3c fd 3c fd fd fd 7d 3c 5d fd fd fd 3c 30 3c fd fd c0 fd 46 fd fd fd 3c 50 fd fd fd fd fd 40 fd 08 fd fd fd 5f 3c fd 3c 40 fd fd 3c fd fd fd 4e 3c fd 3c fd fd fd 62 fd fd fd fd fd fd 3c fd fd fd 60 31 fd 3c 3a fd fd 60 fd fd fd 3c 5d 3c 33 fd fd fd 3c fd fd fd 3c fd 3c fd fd fd 25 fd fd fd fd fd 3c fd fd fd 3c fd 3c 79 fd fd fd fd 27 3c 38 3c 80 fd 44 3c 1a fd fd fd 3c 6c 3c fd fd fd c0 fd 7f fd fd 24 fd 34 17 fd 2f 38 6e fd fd fd 3c 24 3c 60 fd fd 0b fd fd fd 3c 53 3c fd fd fd 34 3c 0c fd fd 28 3c fd 3c 24 fd fd fd fd fd fd fd fd 04 fd fd fd fd fd 58 3c 38 3c 4f fd fd 29 fd fd 6c 3c 68	<X0<:6<&<$-nBC<<}<] <0<F<P_<<<N <<b<`1<:`<]<3<<<% <<<y'<8<D<<l< $4/8n<$<`<S<4<(<<$X<8 <O)l<h	success or wait	6	406224	WriteFile
C:\Users\user\AppData\Local\Temp\ARMOURY CRATE Message.VisualElementsManifest.xml	0	188	3c 41 70 70 6c 69 63 61 74 69 6f 6e 20 78 6d 6c 6e 73 3a 78 73 69 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 2d 69 6e 73 74 61 6e 63 65 22 3e 0d 0a 3c 56 69 73 75 61 6c 45 6c 65 6d 65 6e 74 73 0d 0a 09 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 3d 22 62 6c 61 63 6b 22 0d 0a 09 53 68 6f 77 4e 61 6d 65 4f 6e 53 71 75 61 72 65 31 35 30 78 31 35 30 4c 6f 67 6f 3d 22 6f 6e 22 0d 0a 09 46 6f 72 65 67 72 6f 75 6e 64 54 65 78 74 3d 22 6c 69 67 68 74 22 2f 3e 0d 0a 3c 2f 41 70 70 6c 69 63 61 74 69 6f 6e 3e	<Application xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> <VisualElementsBackgrou u ndColor="black"ShowNameOnSquar e150x150Logo="on"ForegroundText="light"/> </Application>	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\Airplane_14.bmp	0	9184	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 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 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	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\MapiProxy.dll	0	16384	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 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 78 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 24 00 00 50 45 00 00 4c 01 07 00 df 23 62 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 10 00 00 00 1c 00 00 00 00 00 00 60 14 00 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 00 00 00 04 00 00 fd 74 00 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd 27 00 00 fd 00 00 00 fd 28 00 00 64 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL#b"!`t@A'(d	success or wait	2	406224	WriteFile
C:\Users\user\AppData\Local\Temp\Microsoft.Practices.ObjectBuilder2.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 02 00 47 fd 0d 53 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0b 00 00 fd 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 40 01 00 00 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 fd 7d 01 00 03 00 40 fd 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 20 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEdGS" @ }@@@	success or wait	4	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Sports-Wallpapers-1.jpg	0	16384	fd fd fd fd 00 10 4a 46 49 46 00 01 01 01 00 60 00 60 00 00 fd fd 0c 58 49 43 43 5f 50 52 4f 46 49 4c 45 00 01 01 00 00 0c 48 4c 69 6e 6f 02 10 00 00 6d 6e 74 72 52 47 42 20 58 59 5a 20 07 fd 00 02 00 09 00 06 00 31 00 00 61 63 73 70 4d 53 46 54 00 00 00 00 49 45 43 20 73 52 47 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd fd 00 01 00 00 00 00 fd 2d 48 50 20 20 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 63 70 72 74 00 00 01 50 00 00 00 33 64 65 73 63 00 00 01 fd 00 00 00 6c 77 74 70 74 00 00 01 fd 00 00 00 14 62 6b 70 74 00 00 02 04 00 00 00 14 72 58 59 5a 00 00 02 18 00 00 00 14 67 58 59 5a 00 00 02 2c 00 00 00 14 62 58 59 5a 00 00 02 40 00 00 00 14 64	JFIF``XICC_PROFILEHLinomntrRGB XYZ 1acspMSFTIEC sRGB-HP cpr tP3desclwtptbkptrXYZgXYZ,bXYZ@d	success or wait	48	406224	WriteFile
C:\Users\user\AppData\Local\Temp\format-justify-center-symbolic.svg	0	319	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 0a 3c 73 76 67 20 68 65 69 67 68 74 3d 22 31 36 70 78 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 36 20 31 36 22 20 77 69 64 74 68 3d 22 31 36 70 78 22 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 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 6d 20 33 20 32 20 68 20 31 30 20 76 20 32 20 68 20 2d 31 30 20 7a 20 6d 20 30 20 30 22 2f 3e 0a 20 20 20 20 20 20 20 20 3c 70 61 74 68 20 64 3d 22 6d 20 31 2e 30 30 33 39 30 36 20 37 20 68 20 31 34 20 76 20 32 20 68 20 2d 31 34 20 7a 20 6d 20 30 20 30 22 2f 3e 0a	<?xml version="1.0" encoding="UTF-8"?> <svg height="16px" viewBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg"> <g fill="#2e3436"> <path d="m 3 2 h 10 v 2 h -10 z m 0 0"/> <path d="m 1.003906 7 h 14 v 2 h -14 z m 0 0"/>	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fzshellext_64.dll	0	16384	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 50 45 00 00 64 fd 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 2e 22 0b 02 02 23 00 22 00 00 00 48 00 00 00 02 00 00 50 13 00 00 00 10 00 00 00 00 08 67 00 00 00 00 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 fd 00 00 00 04 00 00 40 5e 01 00 03 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd."#"HPg@^`	success or wait	2	406224	WriteFile
C:\Users\user\AppData\Local\Temp\lang-1071.dll	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 3c fd fd fd 52 fd fd fd 52 fd fd fd 52 fd 40 fd fd fd 52 fd 40 fd 50 fd fd fd 52 fd 52 69 63 68 fd fd 52 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 fd 2a 6a 5e 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 00 00 00 00 00 00 74 01 00 00 00 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$<RRR@R@PRRichRPEL*j^!t	success or wait	7	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mail-reply-all-symbolic.symbolic.png	0	244	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd fd fd 3f 6a 42 41 10 fd fd 10 fd 14 29 c0 0a fd 21 3c fd fd fd 0b 79 0a 0f 61 fd 54 09 48 20 fd fd 1b fd fd fd fd fd 67 fd 3c 58 fd fd 1e fd fd 07 5b 7c 33 fd 33 fd fd fd 31 fd 27 fd 06 6f 65 fd fd 28 fd fd fd 56 fd fd fd fd 03 7f fd 5d 7e fd 09 55 fd 34 fd fd fd fd fd 32 fd 5c fd fd 5e fd 05 fd fd 53 fd fd fd 16 fd 3c 39 fd 4f 4c fd 63 fd fd 4b 7c 73 fd 53 fd 57 79 fd 31 fd fd 7c fd fd 55 fd fd 6a 5e 69 12 7b 28 1b fd fd fd 4a fd fd 35 fd 0b 45 34 fd 56 fd f9 01 fd fd 32 fd fd fd 74 11 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dIDAT8?jBA)!<yaTH g<X[|331'oe(V]~U42\^S<9OLcK|s SWy1|Uj^i{(J5E4V2tIENDB`	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\media-playback-start-symbolic.symbolic.png	0	195	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 7a 49 44 41 54 38 fd fd f1 0d fd 50 0c 45 fd 13 1a 26 fd fd 02 fd fd 0c fd fd 65 0a fd 43 0c 02 43 24 52 68 67 72 fd 28 fd 3f 4f fd fd 6d 3d fd fd 14 3c 71 41 fd 15 04 33 4e 58 67 05 fd 03 5d fd 20 18 fd fd 11 14 fd 70 fd 26 2b 08 26 1c fd fd 0a fd fd 6f fd 05 29 fd 09 46 fd 68 fd 0a fd fd 78 fd fd fd fd 3e fd 4b 16 69 fd 51 fd fd 33 92 d4 fd 1b fd fd 61 fd fd 28 6f 3a 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dzIDAT8PE&eC$Rhr(?Om=<qA3NXg] p&+&o)Fhx>KiQ3a(o :IENDB`	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\network-no-route-symbolic.svg	0	1260	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 3c 67 20 66 69 6c 6c 3d 22 23 34 37 34 37 34 37 22 3e 3c 70 61 74 68 20 64 3d 22 4d 31 30 20 31 76 31 63 30 20 2e 32 35 37 2e 31 33 2e 35 32 39 2e 33 31 33 2e 37 31 39 4c 31 31 2e 35 39 33 20 34 48 38 2e 32 33 61 34 2e 30 33 34 20 34 2e 30 33 34 20 30 20 30 31 33 2e 32 37 33 20 32 68 2e 31 32 33 6c 2d 2e 30 37 34 2e 30 37 38 63 2e 32 37 2e 34 39 35 2e 34 34 39 20 31 2e 30 34 37 2e 34 38 32 20 31 2e 36 34 37 6c 2e 30 30 32 2e 30 32 39 76 2e 30 32 37 63 30 20 2e 32 36 35 2d 2e 30 32 31 2e 35 31 36 2d 2e 30 35 32 2e 37 36 32 4c 31 35 2e 34 30 36 20 35 20 31 31 2e 37 35 20	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M10 1v1c0 .257.13.529.313.719L11.593 4H8.23a4.034 4.034 0 013.273 2h.123l-.074.078c.27.495.449 1.047.482 1.647l.002.029v.027c0 .265-.021.516-.052.762L15.406 5 11.75	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\system-reboot-symbolic.symbolic.png	0	327	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd fd 3b 4a 04 41 10 fd fd fd 6a fd 20 1b fd fd 7b fd 78 00 fd 0d 7d 05 7b 07 3d fd fd fd 78 0c 0f fd 28 fd fd fd fd 20 22 18 fd 67 70 55 10 03 5f fd 30 4d 3b 33 2b 58 50 74 fd 57 35 fd fd 6a fd 69 fd 4b fd 0f fd 01 fd fd 4e fd 2c fd fd 0c 63 fd 68 fd fd 64 fd 1c 70 fd 27 2c fd 01 56 fd fd 00 38 fd fd 07 fd fd 4f fd fd 1a 40 2b 19 fd fd fd 14 fd 17 fd fd fd 31 07 fd fd fd 36 53 fd 4d fd fd fd fd 15 2e 32 fd 13 fd e9 fd 16 62 3b fd fd 22 fd fd fd 0a 23 fd fd fd fd 18 4d 0f 25 fd 21 fd fd 3f 00 fd 62 7d 4c 01 fd 58 fd 13 37 55 fd fd 46 fd 0f fd fd 0c 5e 14 23	PNGIHDRasBIT|dIDAT8; JAj {x}{=x("gpU_M;3+XPtW5jiKN,chdp',V8@ +1SM.2b;"#M%!? b}LX7UF^#	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\nsw5376.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 fd 00 00 00 0e 1f fd 0e 00 fd 09 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	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe	unknown	512	success or wait	421	4061F5	ReadFile
C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe	unknown	16384	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsa450D.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsa450D.tmp	unknown	28060	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nsa450D.tmp	unknown	4	success or wait	14	4061F5	ReadFile
C:\Users\user\Desktop\72EED30398363-0983BNDJ0398763536.exe	unknown	16384	success or wait	57	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsa450D.tmp	unknown	16384	success or wait	77	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\TREDIVER.Und	unknown	96538	success or wait	1	732A2C59	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\FLOKDYRS	success or wait	1	406532	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\riffelgangens	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Eyebath	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Eyebath\Qoph28	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Specularity211	success or wait	1	406532	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Specularity211\haandholdt	success or wait	1	406532	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\FLOKDYRS	Fyrvrkeres	dword	0	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\riffelgangens	Spydkasters198	dword	1	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Eyebath\Qoph28	Expand String Value	expand unicode	%WINDIR%\podical.log	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Specularity211\haandholdt	Screwdriver44	unicode	omprioriteret	success or wait	1	40251B	RegSetValueExW

Disassembly

No disassembly