ID: 634111
Sample Name: INVOICE.exe
Cookbook: default.jbs
Time: 16:10:46
Date: 25/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

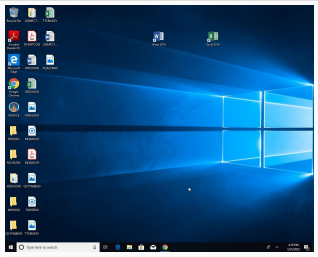
Windows Analysis Report

INVOICE.exe

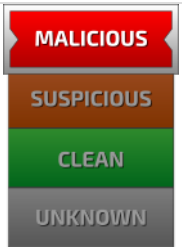
Overview

General Information

Sample Name:	INVOICE.exe
Analysis ID:	634111
MD5:	a10619d494661c..
SHA1:	1273e17b50d8d3.
SHA256:	e126c11aec2897..
Tags:	exe Invoice signed
Infos:	



Detection



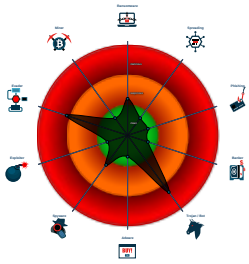
GuLoader

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Initial sample is a PE file and has a…
- Tries to detect virtualization through…
- Executable has a suspicious name …
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- PE file does not import any functions
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- INVOICE.exe (PID: 5860 cmdline: "C:\Users\user\Desktop\INVOICE.exe" MD5: A10619D494661C1F8CA180E53C5A11FD)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://cdn.discordapp.com/attachments/963535165500588126/978282265127825408/NANOBIN_HBsjI150.bin"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.899311337.00000000029F0000.00000040.00001000.00020000.00000000.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

Networking

C2 URLs / IPs found in malware configuration

System Summary

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

Data Obfuscation

Yara detected GuLoader

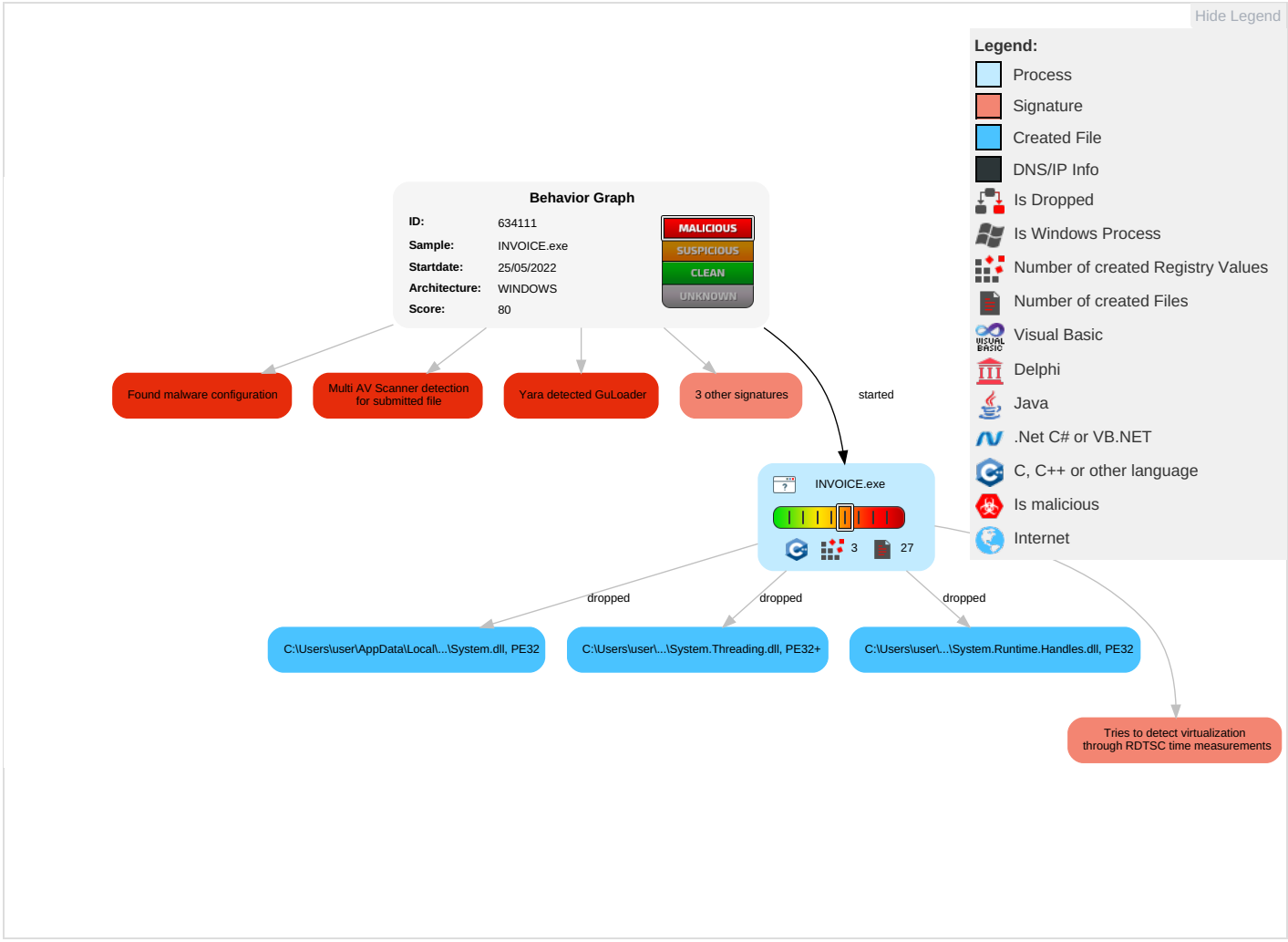
Malware Analysis System Evasion

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 Timestomp	LSASS Memory	4 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)	1 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

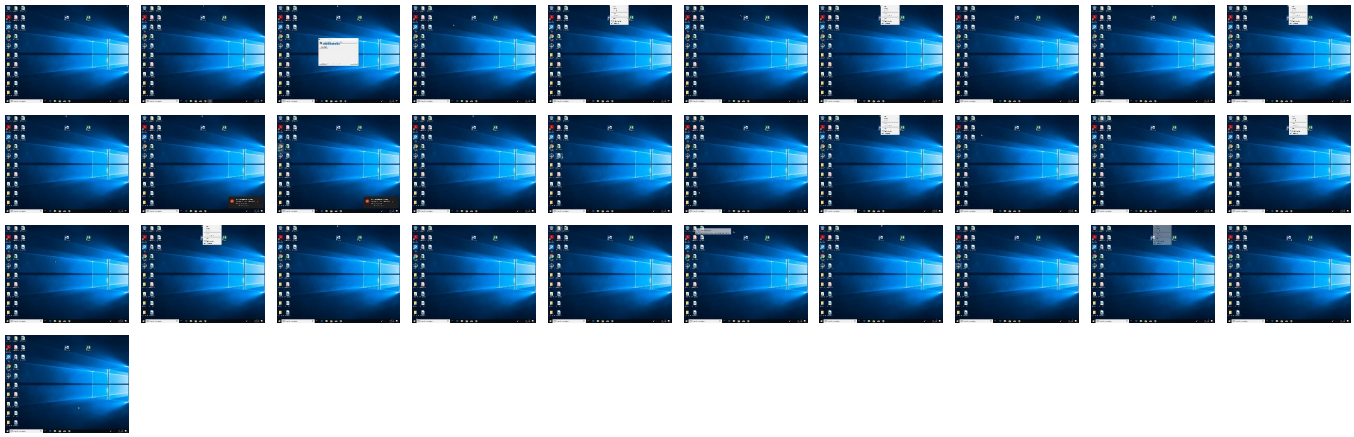
Behavior Graph



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
INVOICE.exe	42%	ReversingLabs	Win32.Trojan.Shelsy	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\System.Runtime.Handles.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\System.Threading.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsg5565.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsg5565.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/963535165500588126/978282265127825408/NANOBIN_HBsjI150.bin	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/dotnet/runtimeBSJB	System.Threading.dll.0.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	INVOICE.exe	false		high
http://mozilla.org/MPL/2.0/.	updater.ini.0.dr	false		high
http://https://github.com/dotnet/runtime	System.Threading.dll.0.dr, System.Runtime.Handles.dll.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	634111
Start date and time: 25/05/202216:10:46	2022-05-25 16:10:46 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INVOICE.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:	18
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:	mal80.troj.evad.winEXE@1/10@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.5% (good quality ratio 84.3%) • Quality average: 86.8% • Quality standard deviation: 21.3%

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, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.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, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.
- VT rate limit hit for: INVOICE.exe

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\Arteriagra2.Syr

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	data
Category:	dropped
Size (bytes):	105748
Entropy (8bit):	6.594105073918034
Encrypted:	false
SSDEEP:	1536:6/oEoq1Iy3Kyat2nSqglaSi+ksT7ewHxgdR:ioEoq1Iy3Kyg6R8aStewRgX
MD5:	6728021C3198EE4F6F422A047AC506EF

<table>
<tr><td>SHA1:</td><td>C2E97C1816BAE3AA7D40C3EA59F52812ED6AAE70</td></tr>
<tr><td>SHA-256:</td><td>4DB076FA62DAEA04C6634069D10E4C7A67846BD1E524B40A989A5C27498BBB98</td></tr>
<tr><td>SHA-512:</td><td>9A3017C4B487F8892E9131EB3452B4A432D997262D169D76133936AB3A5064614F1C3EF93DCE88CE3A84B7BCB5E7D7A3DDA8845DF46D4690A554BDF367FC18D
4</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>Preview:</td><td>...q........6..$G...9.,..||||||||||||||||||||||||||||||||||||||||||||||||||||||.....f.b....4.h..f.....g......*..5o.....................................
.....s.A........4qk./..f..*.....f.c.f.j....(..`F.................................... ....f.f.f.h....%.V...................................{R..f.s....s........'...P.......................................
...c......q..=...H\\\......q.i....f.r.O....3:..}...<.&.svvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
vvvvvvvvvvvvv.................$.W.H...f.... ..0P............................f......f...f...f........!...S444444444444444444444444444444.....f............,.~..ZZZZZ
ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ..f.u..a......!..........................</td></tr>
</table>

C:\Users\user\AppData\Local\Temp\BCGCBProRes_it-IT.nls

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1245
Entropy (8bit):	5.462849750105637
Encrypted:	false
SSDEEP:	24:hM0mIAvy4Wvsqs1Ra7JZRGNeHX+AYcvP2wk1RjdEF3qpMk5:lmIAq1UqsziJZ+eHX+AdP2TvpMk5
MD5:	5343C1A8B203C162A3BF3870D9F50FD4
SHA1:	04B5B886C20D88B57EEA6D8FF882624A4AC1E51D
SHA-256:	DC1D54DAB6EC8C00F70137927504E4F222C8395F10760B6BEECFCFA94E08249F
SHA-512:	E0F50ACB6061744E825A4051765CEBF23E8C489B55B190739409D8A79BB08DAC8F919247A4E5F65A015EA9C57D326BBEF7EA045163915129E01F316C4958D949
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml">..<head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>..<title>404 - File or directory not found.</title>..<style type="text/css">.. ..body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}..fieldset{padding:0 15px 10px 15px;} ..h1{font-size:2.4em;margin:0;color:#FFF;}..h2{font-size:1.7em;margin:0;color:#CC0000;} ..h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} ..#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;..background-color:#555555;}..#content{margin:0 0 0 2%;position:relative;}...content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}..-->..</style>..</head>..<body>..<div id="header"><h1>Server Error</h1></div>..<div id="content">.. <div class="co

C:\Users\user\AppData\Local\Temp\System.Runtime.Handles.dll

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	15512
Entropy (8bit):	6.804862962213531
Encrypted:	false
SSDEEP:	384:PZ152PIWOmWqlC/uPHRN7yYWF//dJR9ztG/+A:R1zSlWMyYWF//dj9zW
MD5:	6CFD24EDAD19285628C42E150B13CEFC
SHA1:	D2349988D62A8047C8194B5C0A25C525B8B58FCB
SHA-256:	C702F48311386BB45B4A9189058914197B16B5B5B9606A39B0F4C24EE891F04E
SHA-512:	1AFA531D42D67BCA0542063DCFB031F06E4CC923F5ADDCD5A954AEEBA03B29EBC37EBD002F6C2CA9144B56D2E3FAD4893C6F3C4C3368D85A5B34F196D1940 980
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...C............"!..0..............)... ....@.. ....;... .`................................x)..S....@..................(...`.......(..8... ....H............text........ ....`.rsrc........@......................@..@.relo c.......`......................@..B.................)......H........ ....P ....$a..*..4t....o.}\Mn..*..q.....o3.l.\w....1..%U.F<...<.s..].j."..?9.N.N...g?.9..'.K.l ..,.].,p.... .4,.M.ly.....p._.LC.MNBSJB............v4.0.30319......`.......#~..L.......#Strings....P.......#GUID...`.......#Blob......................3...(.x.....x...f.F.................'. ....L...........a.......................H.....z.....|.x.................@.....

C:\Users\user\AppData\Local\Temp\System.Threading.dll

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	78952
Entropy (8bit):	6.515753721409949
Encrypted:	false
SSDEEP:	1536:ZFCLZygVO0U5/YrxnU9EqOfxdrJ2RH7AGlUMG:ZyZygVO1exnU9EzxdroKGlUJ

MD5:	514AE47FAB14E04E3F7EF70179184F43
SHA1:	BA17EEA34A75439362C8FB1F12CA438570FBDB77
SHA-256:	3AF3A8B198EADC2120DC9F2CD9AE150EE7BE6F3D0C1985519C3C6E652AD25682
SHA-512:	286ACD03EDD57B36EE72E76995583042B94C244D8C2337DBD63DEB1DA36F5A8D04E0DB6963AB71B033EC442D3C37CF68701B3E4F0A3933E35B111CE9AA8921A6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....." .....0.....{... .`...@.....@..... .....`....)..\.....h$... ..$.....T.....`...H.....text...;..... ..`.data.....@.. ..reloc..$.... .....@..B.....0.....P.....4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....y.....?.....D.....V.a.r.F.i.l.e.I.n.f .o.....$.....T.r.a.n.s.l.a.t.i.o.n.....h.....S.t.r.i.n.g.F.i.l.e.I.n.f.o...D.....0.0.0.0.0.4.b.0...:.....C.o.m.m.e.n.t.s...S.y.s.t.e.m...T.h.r.e.a.d.i.n.g.....L.....C.o.m.p.a.n.y.N.a.m.e.....M.i.c .r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...J.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n.....S.y.s.t.e.m...T.h.r.

C:\Users\user\AppData\Local\Temp\alnicoes.til

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	37546
Entropy (8bit):	3.9997596847051198
Encrypted:	false
SSDEEP:	768:2kQDmlZJu47eyQpLGGDER1k5y93KTddS32yNWhv8LIeYnIxy6F60lZo2/E7J:/fYLvFcPapS3Av8LI+06w0t/G
MD5:	32EA6BDBD368660B87A6EC28764BC17E
SHA1:	A6A680014E0A66AD33D2CB5C8A7797C7CEAC17B5
SHA-256:	63A2C9E2B87F9AFBADB3CB8D66A68C75A0ABD483C05E5FAF24CA57B4E2DE8CC7
SHA-512:	02A6CFBFA9E010252AF19BDD2685D309200B6972C707E0611CCEDE1D28754DFFB3AB0AE67C5260458867B68666A3E55524222B572EA8107B04BC01591AD6B8F
Malicious:	false
Reputation:	low
Preview:	F28AE2E97416D75FE90BB4B3A6736394D00229E223FF26C6428F6CABF02CF5ECF1832FCEE89C461C6522F06F84DEF0379CF3D556372AC3A4613C07F9 DE6B70535D70D7E435B71B70D351DF74E0B191CE46DA8AEB92AF61403721E8A3FF6FD31F18F7196C53A5045CB46A6D6EE4FB17407BE18D3462B12146 9C17677FC65EBB1A38ECC8BB6E105296AE92FA840F814D34EAEED9EE8B1E5260E11AB7D35C6F875DEFB14508B136AE74E476B223879B6849DED035E7 C4D3691BC73CE378CEDF035AE3E7613F8CBED6D3B181DCC17414A5955BB8CECCDE8D44DA68DCC5E07FBECF9EF7FD6AAD072FFC06AA321FB0458FD3D0 5CB8D90DE1726507AC090B852CBE75648DD7BBBA9EC043DC5436EF5BEBFB1EDBCFD129BEA8F2DC3E8A7C8BCDEDEA7F93D75A442478272955AC72F4CA 893C3D7BAFC0B656EDBFED4FE2DDD719DA7513B25E8A3659BA70938CB1F644EE50C5A0E2627A71B87266D6ECF81CEA059605C33F9AEB2F5EEA1CB0DC 3483CE7D929057BB4C44D44DAE1196F0052645EABED4CE08A628ED306334ECB504B93A3975B44F4805517CFCE2B94908D502DBE1C4FEBC8CE1299D4C 136B2DD5699EDD0E99B461425D4661D6F22C483A42900BD2F0EE05D9C684CF691A04B54AA33593A1E7AFD8567E8C60ECA230AFED5D3E95CC7967AC1C 5DE6F1E66B83ECF9A29937C2E28A7B7CE8AF5AE8

C:\Users\user\AppData\Local\Temp\drive-harddisk-usb-symbolic.svg

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	316
Entropy (8bit):	4.795067099691328
Encrypted:	false
SSDEEP:	6:tI9mc4slzcWER4tVvgtt7XR9XeTRnVcMdN/NwWULbm8aBJcllf7lNDME:t4CDqtVvg7XaTRtTFwWULpq8Nl9ME
MD5:	B326D09573739B7BD22AE9BC602BEBE1
SHA1:	6F10B07DF50E425BE75D7C0042E45926CAC06137
SHA-256:	BC31190E955A90C3442F3C222435751717A04834EFB8006334CAC55DA27CAF54
SHA-512:	5C27A1148C50568500133D962A9AFE3E434ED704FC64B9DC42CFBA7F52CABBD35468E8B3096CCFAE0D12EF1D80D710D7B57B98F69677EE5612F8FC39055F925 3
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><path d="M8.5 0h-1l-2 4H7v5H4V7.729A2 2 0 005 6a2 2 0 10-3 1.73V9c0 2 2 2 2 2h3v1.271A2 2 0 006 14a2 2 0 103-1.73V11h3s2 0 2-2V8s1.125-.188 1-1V5c.125-1.125-1-1-1-1h-2c-1.063 0-1 1-1 1v2c0 1 1 1 1 1v1H9V4h1.5z" fill="#2e3436" fill-rule="evenodd"/></svg>

C:\Users\user\AppData\Local\Temp\go-bottom-symbolic.svg

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	710
Entropy (8bit):	4.447432775965755
Encrypted:	false

SSDEEP:	12:TMHdPnnl/nu3tlnuIDLfHShZozWlz2WJhWlz5jJhWlzgbVoJmdJWlzLVoJmdJWlp:2dPnnxu3tlrDLfybcNWv6vLbmJmdJYmZ
MD5:	CF5D546B0985AD2F75E420FDEEE8ABEC
SHA1:	222DC112B47362AA10965C3F98D47951A69CC9D4
SHA-256:	8433D0660B758DC3345BD673251ABA619E9376E92AAA132E1844DCF846F188DA
SHA-512:	D92CB4C6D28DECAE21A065772AABE0A854DDA4EB58C9F425FA6B895949C01F6EF62B461F4F5039712F461AAF5C17673120484EAB581E8ECC688818EB6F5E774E
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 2.707031 2.292969 l -1.414062 1.414062 l 6.707031 6.707031 l 6.707031 -6.707031 l -1.414062 -1.414062 l -5.292969 5.292969 z m 0 0"/>. <path d="m 15 3 v -1 h -1 v 1 z m 0 0"/>. <path d="m 2 3 v -1 h -1 v 1 z m 0 0"/>. <path d="m 3 3 c 0 -0.554688 -0.445312 -1 -1 -1 s -1 0.445312 -1 1 s 0.445312 1 1 1 s 1 -0.445312 1 -1 z m 0 0"/>. <path d="m 15 3 c 0 -0.554688 -0.445312 -1 -1 -1 s -1 0.445312 -1 1 s 0.445312 1 1 1 s 1 -0.445312 1 -1 z m 0 0"/>. <path d="m 1 14 v -2 h 14 v 2 z m 0 0"/>. </g>.</svg>.

C:\Users\user\AppData\Local\Temp\nsg5565.tmp\System.dll

Process:	C:\Users\user\Desktop\INVOICE.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: 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\updater.ini

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	Windows setup INFormation, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	1225
Entropy (8bit):	4.6943702353982895
Encrypted:	false
SSDEEP:	24:ShrmEx6IL6UDUXqk2ba4IkhqHXVvuMQqXzTw0Y1nQXiwnpOU8:S9T0IL6U4S5I2euMtzTw0iQXiwngU8
MD5:	99295D6215590991C85E42E9FAF2761F
SHA1:	FC1C7C55D43FFA7D9CAAC60D248DDC2779ABEBE0
SHA-256:	050A30288F374F867178E9E14FB70192D9A50530E7FE5237A707197EAB028402
SHA-512:	3DE2F860062ED7BD85139B3E0DC9C9388D57A2BECF8731D0550079E19C32AF6EE3578E92C85F42B875C0A55C0682C8105762051996C62D6B77975061198917D9
Malicious:	false
Preview:	; This Source Code Form is subject to the terms of the Mozilla Public.; License, v. 2.0. If a copy of the MPL was not distributed with this.; file, You can obtain one at http://mozilla.org/MPL/2.0/...[Strings].Title=Aggiornamento Firefox.Info=Firefox sta installando gli aggiornamenti e si avvier. fra qualche istante..MozillaMaintenanceDescription=Mozilla Maintenance Service garantisce che sul computer sia sempre installata la versione pi. recente e pi. sicura di Mozilla Firefox. Mantenere Firefox costantemente aggiornato . fondamentale per la sicurezza durante la navigazione, per questo motivo Mozilla consiglia di lasciare attivo questo servizio...; IMPORTANT: This file should always start with a newline in case a locale.; provided updater.ini does not end with a newline..; Application to launch after an update has been successfully applied. This.; must be in the same directory or a sub-directory of the directory of the.; application executable that initiated the software update.

C:\Users\user\AppData\Local\Temp\user-trash-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	164
Entropy (8bit):	5.895691362934477
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBll7Mlgk0zGDPypLCCuCVu9ZcyxDjrIbvcr/bp:6v/lhPyspkhdqLCCuCVuQi/rIbsTp

MD5:	40FD1CB204BCCD773B72525B3FB03265
SHA1:	00745E555F1F69AD74B8926868481658B6DF6DC4
SHA-256:	B7793D587D8D1525BB621C577492C00516A940393105A07C435CBAF01619F8E6
SHA-512:	B74FB1BE2BD317E2F23B395C25D4B38C4E54BE7C67E195E3E5F8697C08DDBFA4ED5F5E33B385993F4AE798CFBAEFD7D249745D5E9E4B3820F14119391A584047
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....[IDAT8.c`@.....WPE.....0.#. Y..\.4..@"I->/..A....`....0.i..P._NDNI...#&+cdi...+z%,.n....IEND.B`.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.238261722532882
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:	INVOICE.exe
File size:	262120
MD5:	a10619d494661c1f8ca180e53c5a11fd
SHA1:	1273e17b50d8d33078df02447fa9adaab255b459
SHA256:	e126c11aec2897bd7959747e70bc85d4153abdadbe45344bb41771ced23f3228
SHA512:	bc1383fa76765e77298ee35d4358bca8b2be7c310d7567f4d93c67790a0f6f03941f1301c11b78bfa5e178dc312ac3d0886417f705e5613f6f732b0b7f23b36a
SSDEEP:	3072:EbG7N2kDTHUpou5I/QGAhsCKgUbnVCP/+B9F9EbvwwgMvdOHcgW0SpC7Pn5r0K85:EbE/HUhO0XI9FWuMvG006yPnfTMR
TLSH:	4F44D020B7A8BB36CCE25DBA057A127E8EE6DE101605DD4327313A4C1A37ED4AF5B215
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...Z.Oa.....j.....

File Icon

Icon Hash:	79c4b6b3b2aae831

Static PE Info

General

Entrypoint:	0x40352d
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:	0x614F9B5A [Sat Sep 25 21:57:46 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="MAGNETOSTATIC FORKORTELSESLISTENS Whizgig ", O=Hereticated, L=Wellsville, S=Kansas, C=US
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	• 5/23/2022 6:06:15 AM 5/23/2023 6:06:15 AM
Subject Chain	• CN="MAGNETOSTATIC FORKORTELSESLISTENS Whizgig ", O=Hereticated, L=Wellsville, S=Kansas, C=US
Version:	3
Thumbprint MD5:	699972A492A19376B77B2AED92BC1C97
Thumbprint SHA-1:	E1F82DA5213EDEC1AB97EC2FFC65EE3DDBD3D55A
Thumbprint SHA-256:	4AFC8697012468A5B106CBE76591E9ADE8C5E8C06F6A3B15A12246F487717BE0
Serial:	DCE6229CB2DDC799

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], 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 00007F97D09E632Ah
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 00007F97D09E62FAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [00434FB8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx

Instruction
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	0x8610	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5f000	0x11320	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x3e7a8	0x1840	.ndata
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	0x6897	0x6a00	False	0.666126179245	data	6.45839821493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a6	0x1600	False	0.439275568182	data	5.02410928126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.521484375	data	4.15458210409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x36000	0x29000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x5f000	0x11320	0x11400	False	0.273027060688	data	4.45026203596	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x5f208	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_DIALOG	0x6fa30	0x100	data	English	United States
RT_DIALOG	0x6fb30	0x11c	data	English	United States
RT_DIALOG	0x6fc50	0xc4	data	English	United States
RT_DIALOG	0x6fd18	0x60	data	English	United States
RT_GROUP_ICON	0x6fd78	0x14	data	English	United States
RT_VERSION	0x6fd90	0x24c	data	English	United States
RT_MANIFEST	0x6ffe0	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import

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, 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	Precept
FileVersion	1.24.4
CompanyName	mimicismudsl
LegalTrademarks	STAV
Comments	Overwashv50
ProductName	SEMI
FileDescription	Bortadopte
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: INVOICE.exe PID: **5860**, Parent PID: **6120**

General

Target ID:	0
Start time:	16:11:59
Start date:	25/05/2022
Path:	C:\Users\user\Desktop\INVOICE.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\INVOICE.exe"
Imagebase:	0x400000
File size:	262120 bytes
MD5 hash:	A10619D494661C1F8CA180E53C5A11FD
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: 00000000.00000002.899311337.00000000029F0000.00000040.00001000.00020000.00000000.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	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nse446C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	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	405AF7	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	405AF7	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	405AF7	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	405AF7	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	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Arteriagra2.Syr	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\BCGCBProRes_it-IT.nls	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\alnicoes.til	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\System.Runtime.Handles.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\System.Threading.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\drive-harddisk-usb-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\go-bottom-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\updater.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\user-trash-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nsg5565.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40609B	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	405AF7	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	405AF7	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	405AF7	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	405AF7	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	405AF7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsg5565.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	405AB7	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsg5565.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406059	CreateFileW
C:\Users\user\AppData\Local\Temp\nsg5565.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	3	406059	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nse446C.tmp	success or wait	1	403875	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsg5565.tmp	success or wait	1	405C78	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\Arteriagra2.Syr	0	27928	fd fd 0f 71 fd 2e 0f fd fd fd fd fd 36 fd fd 24 47 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 fd fd 0f fd fd fd fd fd fd fd fd fd 39 fd 2c fd 0e 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c 7c fd fd fd fd fd 66 0f 62 fd fd fd fd 34 fd 68 fd 03 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 66 fd fd 00 fd 0f 67 fd fd fd fd fd fd 2a 7f fd 35 6f fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd	q.6$G9,|||||||||||||||||||||| ||||||||||||||||||||||||||||||| fb4hfg*5o	success or wait	4	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\BCGCBProRes_it-IT.nls	0	1245	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 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 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/> <title>404 - Fil	success or wait	1	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\alnicoes.til	0	28312	46 32 38 41 45 32 45 39 37 34 31 36 44 37 35 46 45 39 30 42 42 34 42 33 41 36 37 33 36 33 39 34 44 30 30 32 32 39 45 32 32 33 46 46 32 36 43 36 34 32 38 46 36 43 41 42 46 30 32 43 46 35 45 43 46 31 38 33 32 46 43 45 45 38 39 43 34 36 31 43 36 35 32 32 46 30 36 46 38 34 44 45 46 30 33 37 39 43 46 33 44 35 35 36 33 37 32 41 43 33 41 34 36 31 33 43 30 37 46 39 44 45 36 42 37 30 35 33 35 44 37 30 44 37 45 34 33 35 42 37 31 42 37 30 44 33 35 31 44 46 37 34 45 30 42 31 39 31 43 45 34 36 44 41 38 41 45 42 39 32 41 46 36 31 34 30 33 37 32 31 45 38 41 33 46 46 36 46 44 33 31 46 31 38 46 37 31 39 36 43 35 33 41 35 30 34 35 43 42 34 36 41 36 44 36 45 45 34 46 42 31 37 34 30 37 42 45 31 38 44 33 34 36 32 42 31 32 31 34 36 39 43 31 37 36 37 37 46 43 36 35 45 42 42 31	F28AE2E97416D75FE90 BB4B3A67363 94D00229E223FF26C642 8F6CABF02C F5ECF1832FCEE89C461 C6522F06F84 DEF0379CF3D556372AC 3A4613C07F9 DE6B70535D70D7E435B 71B70D351DF 74E0B191CE46DA8AEB 92AF61403721 E8A3FF6FD31F18F7196 C53A5045CB4 6A6D6EE4FB17407BE18 D3462B12146 9C17677FC65EBB1	success or wait	14	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\System.Runtime.Handles.dll	0	15512	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 4c 01 03 00 43 02 fd 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 30 00 00 0a 00 00 00 08 00 00 00 00 00 00 fd 29 00 00 00 20 00 00 00 00 00 00 00 00 40 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 fd 00 00 00 02 00 00 fd 3b 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.$PELC"!0) @ ;`	success or wait	1	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\System.Threading.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 64 fd 03 00 fd 0e fd 00 00 00 00 00 00 00 00 fd 00 22 20 0b 02 0b 00 00 fd 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 fd 01 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 30 01 00 00 02 00 00 fd 7b 01 00 03 00 60 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 00 20 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd" 0{`@@	success or wait	4	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\drive-harddisk-usb-symbolic.svg	0	316	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 70 61 74 68 20 64 3d 22 4d 38 2e 35 20 30 68 2d 31 6c 2d 32 20 34 48 37 76 35 48 34 56 37 2e 37 32 39 41 32 20 32 20 30 20 30 30 35 20 36 61 32 20 32 20 30 20 31 30 2d 33 20 31 2e 37 33 56 39 63 30 20 32 20 32 20 32 20 32 20 32 68 33 76 31 2e 32 37 31 41 32 20 32 20 30 20 30 30 36 20 31 34 61 32 20 32 20 30 20 31 30 33 2d 31 2e 37 33 56 31 31 68 33 73 32 20 30 20 32 2d 32 56 38 73 31 2e 31 32 35 2d 2e 31 38 38 20 31 2d 31 56 35 63 2e 31 32 35 2d 31 2e 31 32 35 2d 31 2d 31 2d 31 2d 31 68 2d 32 63 2d 31 2e 30 36 33 20 30 2d 31 20 31 2d 31 20 31 76 32 63 30 20 31 20 31	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><path d="M8.5 0h-1l-2 4H7v5 H4V7.729A2 2 0 005 6a2 2 0 10-3 1.73V9c0 2 2 2 2 2h3v1.271A2 2 0 006 14a2 2 0 103-1.73V11h 3s2 0 2-2V8s1.125-.188 1-1V5c.125-1.125-1-1-1-1h-2c-1.063 0-1 1-1 1v2c0 1 1	success or wait	1	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\go-bottom-symbolic.svg	0	710	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 32 2e 37 30 37 30 33 31 20 32 2e 32 39 32 39 36 39 20 6c 20 2d 31 2e 34 31 34 30 36 32 20 31 2e 34 31 34 30 36 32 20 6c 20 36 2e 37 30 37 30 33 31 20 36 2e 37 30 37 30 33 31 20 6c 20 36 2e 37 30 37 30 33 31 20 2d 36 2e 37 30 37 30 33 31 20 6c 20 2d 31 2e 34	<?xml version="1.0" encoding="UTF-8"?> <svg height="16px" vieBox="0 0 16 16" width="16px" xmlns="http://www.w3.org/2000/svg"> <g fill="#2e3436"> <path d="m 2.707031 2.292969 l -1.414062 1.414062 l 6.707031 6.707031 l 6.707031 -6.707031 l -1.4	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\updater.ini	0	1225	3b 20 54 68 69 73 20 53 6f 75 72 63 65 20 43 6f 64 65 20 46 6f 72 6d 20 69 73 20 73 75 62 6a 65 63 74 20 74 6f 20 74 68 65 20 74 65 72 6d 73 20 6f 66 20 74 68 65 20 4d 6f 7a 69 6c 6c 61 20 50 75 62 6c 69 63 0a 3b 20 4c 69 63 65 6e 73 65 2c 20 76 2e 20 32 2e 30 2e 20 49 66 20 61 20 63 6f 70 79 20 6f 66 20 74 68 65 20 4d 50 4c 20 77 61 73 20 6e 6f 74 20 64 69 73 74 72 69 62 75 74 65 64 20 77 69 74 68 20 74 68 69 73 0a 3b 20 66 69 6c 65 2c 20 59 6f 75 20 63 61 6e 20 6f 62 74 61 69 6e 20 6f 6e 65 20 61 74 20 68 74 74 70 3a 2f 2f 6d 6f 7a 69 6c 6c 61 2e 6f 72 67 2f 4d 50 4c 2f 32 2e 30 2f 2e 0a 0a 5b 53 74 72 69 6e 67 73 5d 0a 54 69 74 6c 65 3d 41 67 67 69 6f 72 6e 61 6d 65 6e 74 6f 20 46 69 72 65 66 6f 78 0a 49 6e 66 6f 3d 46 69 72 65 66 6f 78 20 73 74 61 20	; This Source Code Form is subject to the terms of the Mozilla Public; License, v. 2.0. If a copy of the MPL was not distributed with this; file, You can obtain one at http://mozilla.org/MPL/2.0/. [Strings]Title =Aggiornamento FirefoxInfo=Firefox sta	success or wait	1	4060F9	WriteFile
C:\Users\user\AppData\Local\Temp\user-trash-symbolic.symbolic.png	0	164	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 5b 49 44 41 54 38 fd 63 60 40 05 fd 0c 0c 0c fd 18 18 18 fd fd fd fd fd 02 57 50 45 fd fd 7f 06 06 fd fd 30 0e 23 fd 20 59 fd fd 5c fd 34 01 fd 40 22 49 2d 3e 2f fd fd 41 fd 00 fd fd 60 fd 00 fd 06 30 fd 69 fd fd 50 1a 5f 4e 44 4e 6c fd fd 0d 23 26 2b 63 64 69 00 fd fd 2b 7a 25 2c fd 6e 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|d[IDAT8c`@WPE0# Y\4@"I->/A`0iP_NDNI#&+cdi+z%,nIENDB`	success or wait	1	4060F9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsg5565.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 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	4060F9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\INVOICE.exe	unknown	512	success or wait	214	4060CA	ReadFile
C:\Users\user\Desktop\INVOICE.exe	unknown	4	success or wait	2	4060CA	ReadFile
C:\Users\user\Desktop\INVOICE.exe	unknown	4	success or wait	42	4060CA	ReadFile
C:\Users\user\AppData\Local\Temp\alnicoes.til	unknown	2	success or wait	1023	40275E	ReadFile
C:\Users\user\Desktop\INVOICE.exe	unknown	4	success or wait	2	4060CA	ReadFile
C:\Users\user\AppData\Local\Temp\Arteriagra2.Syr	unknown	1048576	success or wait	1	73542C59	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\heliolitidae	success or wait	1	406407	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\neoplatonic	success or wait	1	406407	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\neoplatonic\Harlekinsommerfugl6	success or wait	1	406407	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Sptte210	success or wait	1	406407	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Sptte210\Prjudicerer211	success or wait	1	406407	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\heliolitidae	Tndt228	dword	0	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\neoplatonic\Harlekinsommerfugl6	unportentous	unicode	udsparede	success or wait	1	40251B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Sptte210\Prjudicerer211	Expand String Value	expand unicode	%WINDIR%\TPPEBELAGTES.log	success or wait	1	40251B	RegSetValueExW

Disassembly

No disassembly