ID: 831163
Sample Name: Autoplay.exe
Cookbook: default.jbs
Time: 07:15:11
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

Copyright Joe Security LLC 2023

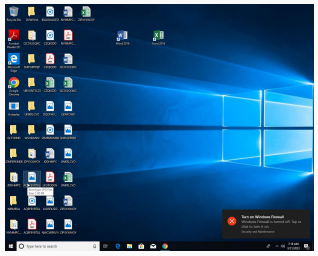
Windows Analysis Report

Autoplay.exe

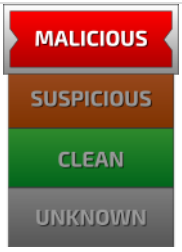
Overview

General Information

Sample Name:	Autoplay.exe
Analysis ID:	831163
MD5:	66ac9ab5cd38…
SHA1:	6671c3205779…
SHA256:	1f9bd27fd7591…
Tags:	exe malware stealer
Infos:	



Detection



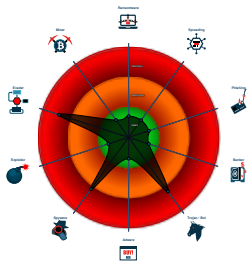
LummaC Stealer

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

Signatures

- Yara detected LummaC Stealer
- Multi AV Scanner detection for subm…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Hides threads from debuggers
- Overwrites code with unconditional j…
- Tries to evade analysis by executio…
- Tries to detect virtualization through…
- Found potential dummy code loops …
- Machine Learning detection for sam…
- Tries to harvest and steal browser in…
- PE file contains section with specia…

Classification



Process Tree

- **System is w10x64**
- Autoplay.exe (PID: 1400 cmdline: C:\Users\user\Desktop\Autoplay.exe MD5: 66AC9AB5CD3881B7799A8CEC1C6611F0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.574486828.0000000000401000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_LummaCStealer	Yara detected LummaC Stealer	Joe Security	
Process Memory Space: Autoplay.exe PID: 1400	JoeSecurity_LummaCStealer	Yara detected LummaC Stealer	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Autoplay.exe.3c0000.0.unpack	JoeSecurity_LummaCStealer	Yara detected LummaC Stealer	Joe Security	

Copyright Joe Security LLC 2023

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

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

System Summary

PE file contains section with special chars

Hooking and other Techniques for Hiding and Protection

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

Malware Analysis System Evasion

Tries to evade analysis by execution special instruction (VM detection)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging

Hides threads from debuggers

Found potential dummy code loops (likely to delay analysis)

Stealing of Sensitive Information

Yara detected LummaC Stealer

Tries to harvest and steal browser information (history, passwords, etc)

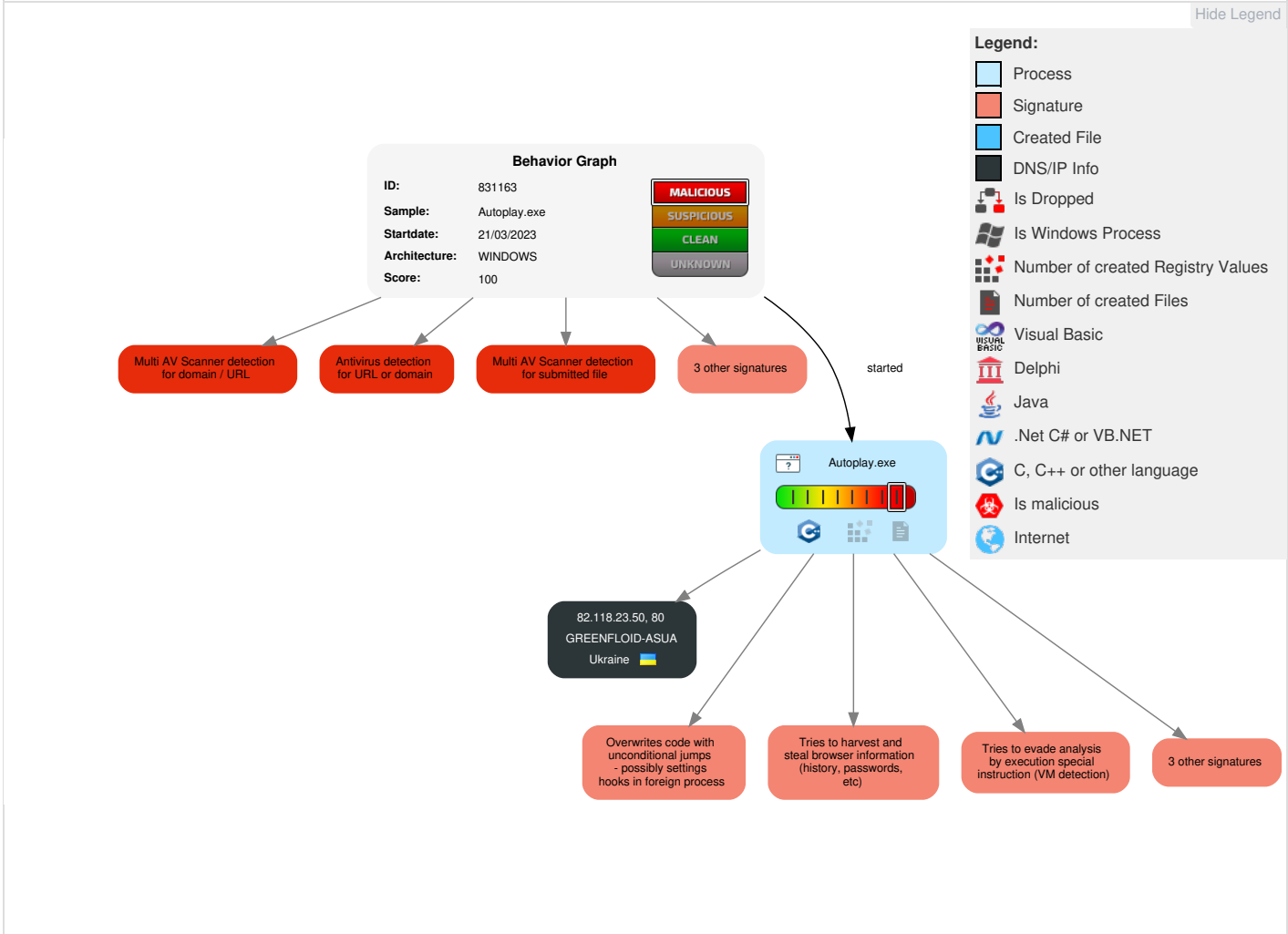
Remote Access Functionality

Yara detected LummaC Stealer

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	Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	2 2 1 Virtualization/Sandbox Evasion	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Credential API Hooking	4 2 1 Security Software Discovery	Remote Desktop Protocol	1 1 Data from Local System	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	2 2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	2 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

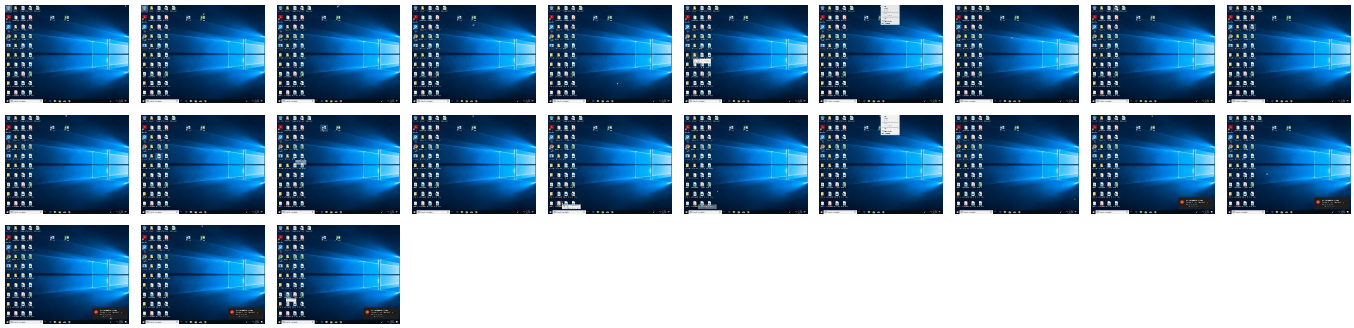
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Autoplay.exe	26%	ReversingLabs	Win32.Trojan.Generic	
Autoplay.exe	26%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
Autoplay.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.Autoplay.exe.3c0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.Autoplay.exe.3c0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://82.118.23.50/c2socksBi	100%	Avira URL Cloud	malware	
http://82.118.23.50/	100%	Avira URL Cloud	malware	
http://82.118.23.50/c2sockYi	100%	Avira URL Cloud	malware	
http://82.118.23.50/c2socksSi	100%	Avira URL Cloud	malware	
http://82.118.23.50/c2sock	100%	Avira URL Cloud	malware	
http://82.118.23.50/c2sock	13%	Virustotal		Browse
http://82.118.23.50/	9%	Virustotal		Browse

Domains and IPs

Contacted Domains

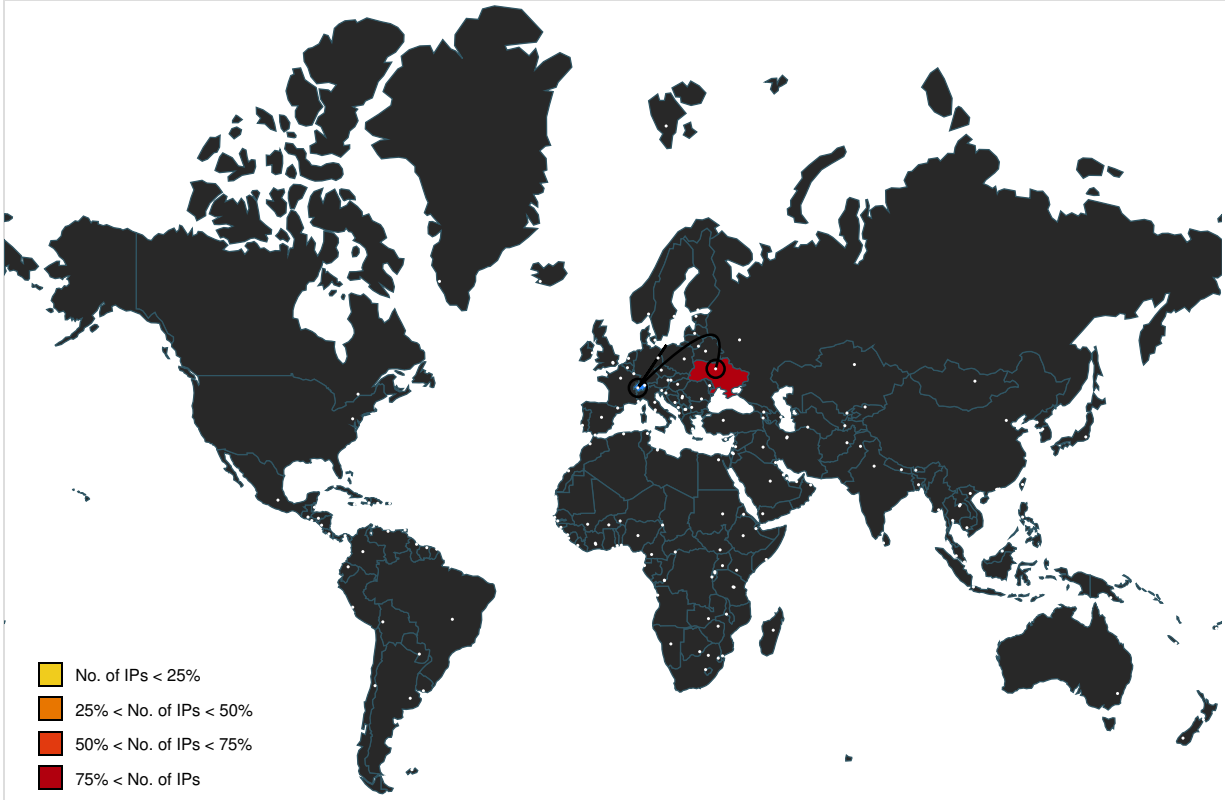
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://82.118.23.50/c2sock	Autoplay.exe, Autoplay.exe, 00000000.00000002.581255406.00000000037AA000.00000004.00000020.00020000.00000000.sdmp, Autoplay.exe, 00000000.00000002.581825210.0000000003FA6000.00000004.00000020.00020000.00000000.sdmp	false	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://ac.ecosia.org/autocomplete?q=	Autoplay.exe, 00000000.00000003.330780726.000000000376E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfp	Autoplay.exe, 00000000.00000003.330780726.000000000376E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://82.118.23.50/	Autoplay.exe, 00000000.00000002.581825210.0000000003F9F000.00000004.00000020.00020000.00000000.sdmp	false	• 9%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://duckduckgo.com/chrome_newtab	Autoplay.exe, 00000000.00000003.330780726.000000000376E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://82.118.23.50/c2socksSi	Autoplay.exe, 00000000.00000002.581825210.0000000003FA6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://duckduckgo.com/ac/?q=	Autoplay.exe, 00000000.00000003.330780726.000000000376E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	Autoplay.exe, 00000000.00000003.330780726.000000000376E000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://search.yahoo.com?fr=crmas_sfpf	Autoplay.exe, 00000000.00000003.33078072 6.000000000376E000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://82.118.23.50/c2sockYi	Autoplay.exe, 00000000.00000002.58182521 0.0000000003FA6000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	Autoplay.exe, 00000000.00000003.33078072 6.000000000376E000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://r.acdsee.com/Ot1su=Copy	Autoplay.exe, 00000000.00000002.58076631 5.000000000116D000.00000002.00000001.010 00000.00000003.sdmp	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	Autoplay.exe, 00000000.00000003.33078072 6.000000000376E000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	Autoplay.exe, 00000000.00000003.33078072 6.000000000376E000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	Autoplay.exe, 00000000.00000003.33078072 6.000000000376E000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://82.118.23.50/c2socksBi	Autoplay.exe, 00000000.00000002.58182521 0.0000000003FA6000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
82.118.23.50	unknown	Ukraine		204957	GREENFLOID-ASUA	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	831163
Start date and time:	2023-03-21 07:15:11 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 35s

Copyright Joe Security LLC 2023

Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	6
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
Sample file name:	Autoplay.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@1/0@0/1
EGA Information:	Failed
HDC Information:	Failed
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

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Execution Graph export aborted for target Autoplay.exe, PID 1400 because there are no executed function
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.972883600683515
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:	Autoplay.exe
File size:	7896576
MD5:	66ac9ab5cd3881b7799a8cec1c6611f0
SHA1:	6671c3205779264e90cfbb17221f62a31aef8d4c
SHA256:	1f9bd27fd7591a98afd67499ae6730eb56c137335d283892bc06b7ab2241ed6c
SHA512:	822767088e411ef88f9ab4d2c400a5ece7793088993fef45ae1e437ad1a1902342faf4eb1cef879b1d20a3d6e36b1eea2512544db4a7c203dcf504dde92e9efd
SSDEEP:	196608:57bHTT6IwW0srdF31vvetKgMU3zClYEcuSGNP:p7/6NWbdR1vvkDH3elV4u
TLSH:	5186332312E90199E2E7CC35C92BBDA877F953177A43EC7855DAADC03A154F4A203B47
File Content Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...>..d....."".....tf.....@.....p.....G.y...@.....E.O...."_....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0xa674a6
Entrypoint Section:	.!Q:
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, TERMINAL_SERVER_AWARE
Time Stamp:	0x6405063E [Sun Mar 5 21:14:38 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	201158e51d2f48f39b5bd36ba20e0af4

Entrypoint Preview

Instruction
push 2AA570F6h
not dword ptr [esp+00h]

Instruction
pushfd
and word ptr [esp+04h], 3854h
neg dword ptr [esp+04h]
not byte ptr [esp+04h]
push ebp
mov ebp, dword ptr [esp+08h]
sub bp, 671Bh
cmp dword ptr [esp+08h], 09827516h
push edx
push ecx
call 00007F40609E7106h
mov bl, FCh
pop esp
add dword ptr [ecx+42769810h], edi
sub edx, dword ptr [ebp+67h]
cmp ebx, esp
stosd
push edx
cmp eax, A0BDD9B2h
pop edx
mov eax, edi
jnl 00007F4060A6B1E9h
pop esi
retf
inc edx
push cs
jecxz 00007F4060A6B15Ch
imul esi, dword ptr [edi-2F607FA2h], FCFEF753h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x45d504	0xc4f	.!Q:
IMAGE_DIRECTORY_ENTRY_IMPORT	0x5f2280	0xa0	.!Q:
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb97000	0x21fbae	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb96000	0x6b0	.reloc
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	0xb955f0	0xc0	.!Q:
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x410000	0x50	.oLB
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	0x3fcc1	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x41000	0xaf24	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x4c000	0x1900	0xc00	False	0.15983072916666666	OpenPGP Public Key	2.010701138279006	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Copyright Joe Security LLC 2023

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.00cfg	0x4e000	0x8	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.voltbl	0x4f000	0x34	0x200	False	0.126953125	data	0.9466526631761399	
.I6g	0x50000	0x3bfac5	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.oLB	0x410000	0x4d0	0x600	False	0.049479166666666664	PGP symmetric key encrypted data - Plaintext or unencrypted data	0.30101446454312897	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.!Q:	0x411000	0x7846b0	0x784800	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.reloc	0xb96000	0x6b0	0x800	False	0.4638671875	data	3.9930181850505764	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xb97000	0x21fbae	0x1600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0xb985e0	0x4ee8	data	English	Canada
RT_BITMAP	0xb9d4c8	0x4b2a	empty	English	Canada
RT_BITMAP	0xba1ff4	0x4ee8	empty	English	Canada
RT_BITMAP	0xba6edc	0x48	empty	English	Canada
RT_BITMAP	0xba6f24	0x4c	empty	English	Canada
RT_BITMAP	0xba6f70	0x4ee8	empty	English	Canada
RT_BITMAP	0xbabe58	0x7b98	empty	English	Canada
RT_BITMAP	0xbb39f0	0xb158	empty	English	Canada
RT_BITMAP	0xbbeb48	0x13b28	empty	English	Canada
RT_BITMAP	0xbd2670	0x7b98	empty	English	Canada
RT_BITMAP	0xbda208	0xb158	empty	English	Canada
RT_BITMAP	0xbe5360	0x13b28	empty	English	Canada
RT_BITMAP	0xbf8e88	0x7b98	empty	English	Canada
RT_BITMAP	0xc00a20	0xb158	empty	English	Canada
RT_BITMAP	0xc0bb78	0x13b28	empty	English	Canada
RT_BITMAP	0xc1f6a0	0x755a	empty	English	Canada
RT_BITMAP	0xc26bfc	0xa8ea	empty	English	Canada
RT_BITMAP	0xc314e8	0x12c2a	empty	English	Canada
RT_BITMAP	0xc44114	0x24568	empty	English	Canada
RT_BITMAP	0xc6867c	0x38d88	empty	English	Canada
RT_BITMAP	0xca1404	0x51bf8	empty	English	Canada
RT_BITMAP	0xcf2ffc	0x91528	empty	English	Canada
RT_BITMAP	0xd84524	0x4b2a	empty	English	Canada
RT_BITMAP	0xd89050	0x755a	empty	English	Canada
RT_BITMAP	0xd905ac	0xa8ea	empty	English	Canada
RT_BITMAP	0xd9ae98	0x12c2a	empty	English	Canada
RT_MENU	0xdadac4	0x4a	empty	English	United States
RT_MENU	0xdadb10	0x70	empty	English	United States
RT_MENU	0xdadb80	0x1014	empty	English	United States
RT_MENU	0xdaeb94	0x172	empty	English	United States
RT_DIALOG	0xdaed08	0x1b0	empty	English	Canada
RT_DIALOG	0xdaeeb8	0xee	empty	English	United States
RT_DIALOG	0xdaefa8	0x10a	empty	English	United States
RT_DIALOG	0xdaf0b4	0xfc	empty	English	United States
RT_DIALOG	0xdaf1b0	0x9c	empty	English	United States
RT_DIALOG	0xdaf24c	0x110	empty	English	United States
RT_DIALOG	0xdaf35c	0xfc	empty	English	United States
RT_DIALOG	0xdaf458	0x130	empty	English	United States
RT_DIALOG	0xdaf588	0x248	empty	English	United States

Copyright Joe Security LLC 2023

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0xdaf7d0	0x106	empty	English	United States
RT_DIALOG	0xdaf8d8	0x260	empty	English	United States
RT_DIALOG	0xdafb38	0x488	empty	English	United States
RT_DIALOG	0xdaffc0	0x2fc	empty	English	United States
RT_DIALOG	0xdb02bc	0x2fc	empty	English	United States
RT_DIALOG	0xdb05b8	0x2fc	empty	English	United States
RT_DIALOG	0xdb08b4	0x2bc	empty	English	United States
RT_DIALOG	0xdb0b70	0x2fc	empty	English	United States
RT_DIALOG	0xdb0e6c	0x2fc	empty	English	United States
RT_DIALOG	0xdb1168	0x1da	empty	English	United States
RT_STRING	0xdb1344	0x1d2	empty	English	United States
RT_STRING	0xdb1518	0x330	empty	English	United States
RT_STRING	0xdb1848	0x13c0	empty	English	United States
RT_STRING	0xdb2c08	0x3bc	empty	English	United States
RT_STRING	0xdb2fc4	0x42	empty	English	United States
RT_STRING	0xdb3008	0x1bc	empty	English	United States
RT_STRING	0xdb31c4	0x80	empty	English	United States
RT_STRING	0xdb3244	0x2c	empty	English	United States
RT_STRING	0xdb3270	0x2d8	empty	English	United States
RT_STRING	0xdb3548	0xb0	empty	English	United States
RT_STRING	0xdb35f8	0xd8	empty	English	United States
RT_STRING	0xdb36d0	0x36	empty	English	United States
RT_STRING	0xdb3708	0x11e	empty	English	United States
RT_STRING	0xdb3828	0xba	empty	English	United States
RT_STRING	0xdb38e4	0x4b6	empty	English	United States
RT_STRING	0xdb3d9c	0x172	empty	English	United States
RT_STRING	0xdb3f10	0x136	empty	English	United States
RT_STRING	0xdb4048	0x13a	empty	English	United States
RT_STRING	0xdb4184	0x360	empty	English	United States
RT_STRING	0xdb44e4	0x18e	empty	English	United States
RT_STRING	0xdb4674	0x356	empty	English	United States
RT_STRING	0xdb49cc	0x372	empty	English	United States
RT_STRING	0xdb4d40	0x9a	empty	English	United States
RT_STRING	0xdb4ddc	0x16e	empty	English	United States
RT_STRING	0xdb4f4c	0x100	empty	English	United States
RT_STRING	0xdb504c	0x188	empty	English	United States
RT_STRING	0xdb51d4	0x10a	empty	English	United States
RT_STRING	0xdb52e0	0x1be	empty	English	United States
RT_STRING	0xdb54a0	0x324	empty	English	United States
RT_STRING	0xdb57c4	0x48c	empty	English	United States
RT_STRING	0xdb5c50	0x234	empty	English	United States
RT_STRING	0xdb5e84	0x602	empty	English	United States
RT_STRING	0xdb6488	0x29a	empty	English	United States
RT_STRING	0xdb6724	0x416	empty	English	United States
RT_STRING	0xdb6b3c	0x48	empty	English	United States
RT_STRING	0xdb6b84	0x2a	empty	English	United States
RT_VERSION	0xb980f0	0x3ac	data	English	Canada
RT_MANIFEST	0xb9849c	0x143	XML 1.0 document, ASCII text	English	United States

Imports

DLL	Import
KERNEL32.dll	CloseHandle
ADVAPI32.dll	GetUserNameW
USER32.dll	EnumDisplayDevicesA
GDI32.dll	BitBlt
KERNEL32.dll	GetSystemTimeAsFileTime
USER32.dll	CharUpperBuffW
KERNEL32.dll	LocalAlloc, LocalFree, GetModuleFileNameW, ExitProcess, LoadLibraryA, GetModuleHandleA, GetProcAddress

Copyright Joe Security LLC 2023

Possible Origin		
Language of compilation system	**Country where language is spoken**	**Map**
English	Canada	
English	United States	

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 07:16:18.173217058 CET	49692	80	192.168.2.4	82.118.23.50
Mar 21, 2023 07:16:21.338139057 CET	49692	80	192.168.2.4	82.118.23.50
Mar 21, 2023 07:16:27.447103024 CET	49692	80	192.168.2.4	82.118.23.50
Mar 21, 2023 07:16:40.245229006 CET	49696	80	192.168.2.4	82.118.23.50
Mar 21, 2023 07:16:43.245233059 CET	49696	80	192.168.2.4	82.118.23.50
Mar 21, 2023 07:16:49.245976925 CET	49696	80	192.168.2.4	82.118.23.50
Mar 21, 2023 07:17:02.131855965 CET	49697	80	192.168.2.4	82.118.23.50
Mar 21, 2023 07:17:05.137738943 CET	49697	80	192.168.2.4	82.118.23.50
Mar 21, 2023 07:17:11.138310909 CET	49697	80	192.168.2.4	82.118.23.50
Mar 21, 2023 07:17:24.014873981 CET	49698	80	192.168.2.4	82.118.23.50
Mar 21, 2023 07:17:27.014650106 CET	49698	80	192.168.2.4	82.118.23.50
Mar 21, 2023 07:17:33.015050888 CET	49698	80	192.168.2.4	82.118.23.50
Mar 21, 2023 07:17:45.045954943 CET	49699	80	192.168.2.4	82.118.23.50
Mar 21, 2023 07:17:48.047540903 CET	49699	80	192.168.2.4	82.118.23.50
Mar 21, 2023 07:17:54.110579014 CET	49699	80	192.168.2.4	82.118.23.50
Mar 21, 2023 07:18:06.183335066 CET	49700	80	192.168.2.4	82.118.23.50
Mar 21, 2023 07:18:09.181503057 CET	49700	80	192.168.2.4	82.118.23.50

Statistics

No statistics

System Behavior

Analysis Process: Autoplay.exe PID: **1400**, Parent PID: **3528**

General

Target ID:	0
Start time:	07:16:04
Start date:	21/03/2023
Path:	C:\Users\user\Desktop\Autoplay.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Autoplay.exe
Imagebase:	0x3c0000
File size:	7896576 bytes
MD5 hash:	66AC9AB5CD3881B7799A8CEC1C6611F0

Copyright Joe Security LLC 2023

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_LummaCStealer, Description: Yara detected LummaC Stealer, Source: 00000000.00000002.574486828.0000000000401000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	61167	success or wait	2	3CB64F	NtReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	unknown	147456	success or wait	2	3CB64F	NtReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	3CB64F	NtReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data For Account	unknown	47104	success or wait	1	3CB64F	NtReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	94208	success or wait	1	3CB64F	NtReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	28672	success or wait	1	3CB64F	NtReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	unknown	10416	success or wait	1	3CB64F	NtReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\CURRENT	unknown	16	success or wait	1	3CB64F	NtReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	unknown	332	success or wait	1	3CB64F	NtReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old	unknown	329	success or wait	1	3CB64F	NtReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\MANIFEST-000001	unknown	41	success or wait	1	3CB64F	NtReadFile

Disassembly

No disassembly

Copyright Joe Security LLC 2023