

JOeSandbox Cloud BASIC



ID: 432748

Sample Name: G9xXUq625O

Cookbook: default.jbs

Time: 18:08:15

Date: 10/06/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report G9xXUq625O	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Agenttesla	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	4
Sigma Overview	5
Signature Overview	5
AV Detection:	5
Compliance:	5
Spam, unwanted Advertisements and Ransom Demands:	5
System Summary:	5
Data Obfuscation:	5
Malware Analysis System Evasion:	5
HIPS / PFW / Operating System Protection Evasion:	5
Lowering of HIPS / PFW / Operating System Security Settings:	6
Stealing of Sensitive Information:	6
Remote Access Functionality:	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	10
Contacted Domains	10
URLs from Memory and Binaries	10
Contacted IPs	10
General Information	10
Simulations	11
Behavior and APIs	11
Joe Sandbox View / Context	11
IPs	11
Domains	11
ASN	11
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	12
Static File Info	12
General	12
File Icon	13
Static PE Info	13
General	13
Entrypoint Preview	13
Data Directories	13
Sections	13
Resources	13
Imports	13
Version Infos	13
Network Behavior	13
Code Manipulations	14
Statistics	14
Behavior	14
System Behavior	14
Analysis Process: G9xXUq625O.exe PID: 6320 Parent PID: 5880	14
General	14
File Activities	14
File Created	14
File Written	14
File Read	14
Analysis Process: G9xXUq625O.exe PID: 7144 Parent PID: 6320	14
General	14
File Activities	15
File Created	15

File Written	15
File Read	15
Disassembly	15
Code Analysis	15

Analysis Report G9xXUq625O

Overview

General Information

Sample Name:

G9xXUq625O (renamed file extension from none to exe)

Analysis ID:

432748

MD5:

9a188a4b5ab76f5.

SHA1:

b61e66760f0959f..

SHA256:

12b582ab21f7f9c..

Tags:

AgentTesla

exe

trojan

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

AgentTesla

Score:

100

Range:

0 - 100

Whitelisted:

false

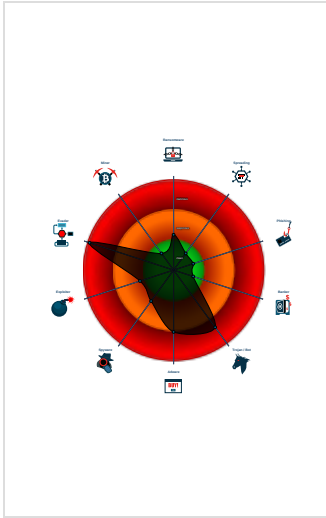
Confidence:

100%

Signatures

- Detected unpacking (changes PE se...
- Detected unpacking (overwrites its o...
- Found malware configuration
- Multi AV Scanner detection for subm...
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg...
- Injects a PE file into a foreign proce...
- Modifies the hosts file
- Queries sensitive BIOS Information ...
- Queries sensitive network adapter in...

Classification



Process Tree

- System is w10x64
- G9xXUq625O.exe (PID: 6320 cmdline: 'C:\Users\user\Desktop\G9xXUq625O.exe' MD5: 9A188A4B5AB76F5D53892F7BCD5DFBEB)
 - G9xXUq625O.exe (PID: 7144 cmdline: {path} MD5: 9A188A4B5AB76F5D53892F7BCD5DFBEB)
- cleanup

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "macslog@lontor.cf7213575aceACE@#$lontor.cfmacs@lontor.cf"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000000.425863712.0000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000000.425863712.0000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.431520750.000000000426 A000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.431520750.000000000426 A000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.429711902.000000000326 3000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Click to see the 8 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.G9xXUq625O.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
9.2.G9xXUq625O.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
9.0.G9xXUq625O.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
9.0.G9xXUq625O.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.G9xXUq625O.exe.432b7f8.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

 Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Compliance:



Detected unpacking (overwrites its own PE header)

Spam, unwanted Advertisements and Ransom Demands:



Modifies the hosts file

System Summary:



.NET source code contains very large array initializations

Data Obfuscation:



Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Malware Analysis System Evasion:



Yara detected AntiVM3

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:



Injects a PE file into a foreign processes

Modifies the hosts file

Lowering of HIPS / PFW / Operating System Security Settings:



Modifies the hosts file

Stealing of Sensitive Information:



Yara detected AgentTesla

Yara detected AgentTesla

Remote Access Functionality:



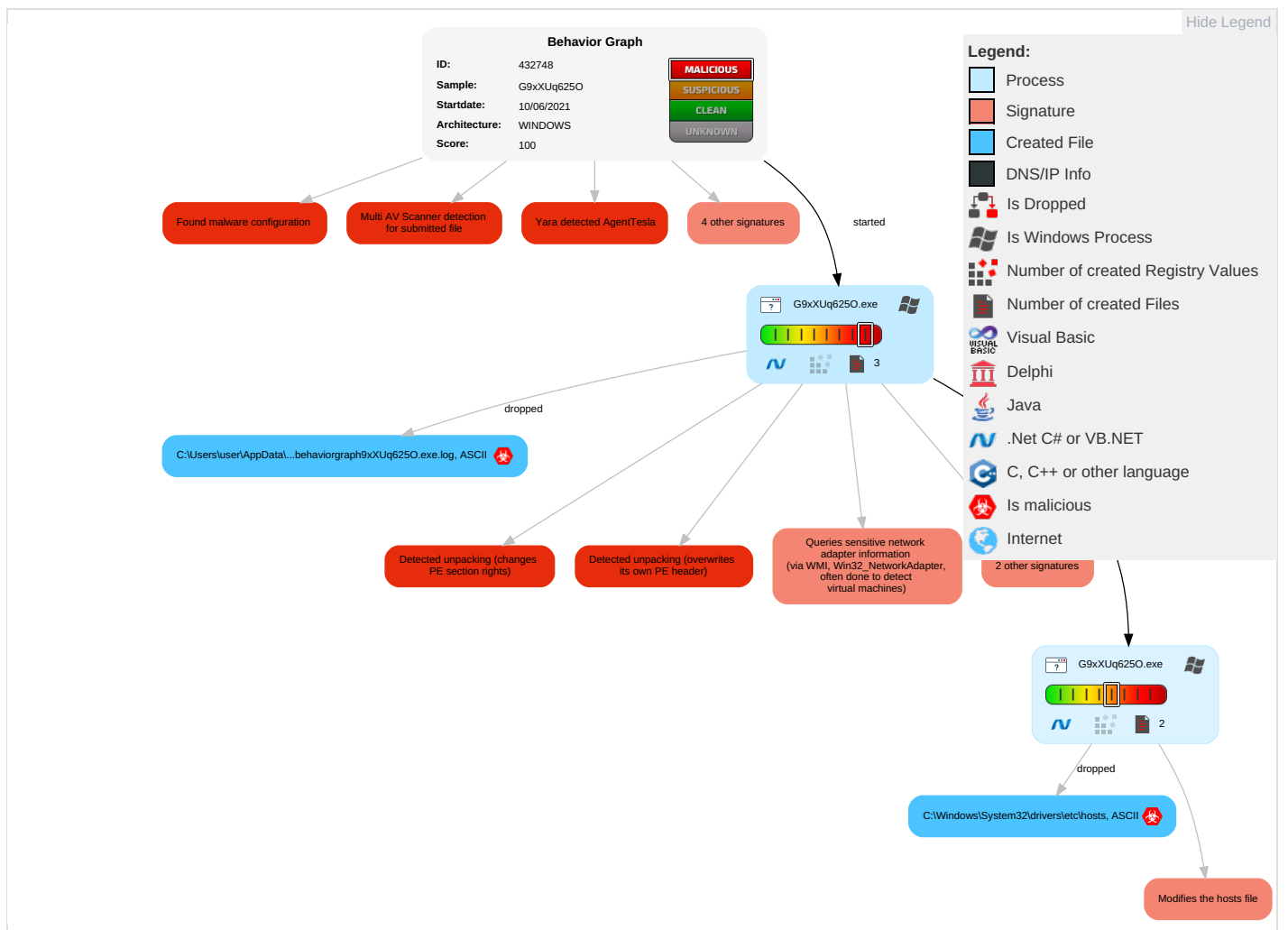
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	File and Directory Permissions Modification 1	LSASS Memory	Security Software Discovery 2 1 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 1 3 1	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

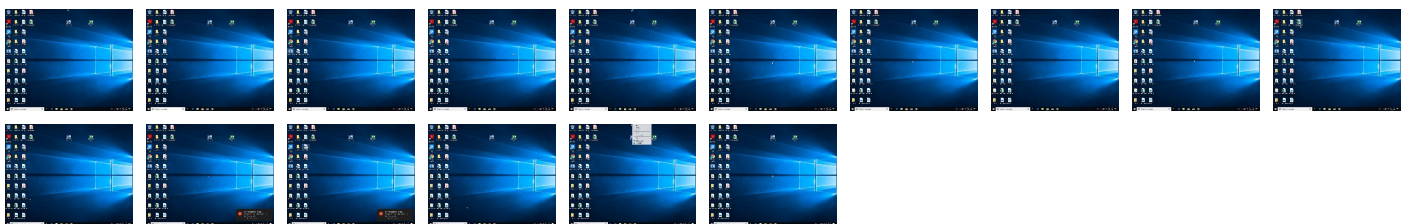
Behavior Graph



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
G9xXUq625O.exe	32%	Virustotal		Browse
G9xXUq625O.exe	39%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.G9xXUq625O.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.G9xXUq625O.exe.e50000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
9.2.G9xXUq625O.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnO	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnN	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.sandoll.co.krFd	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnG	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnC	0%	URL Reputation	safe	
http://www.founder.com.cn/cnC	0%	URL Reputation	safe	
http://www.founder.com.cn/cnC	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.sandoll.co.krY	0%	Avira URL Cloud	safe	
http://www.urwpp.deoi	0%	Avira URL Cloud	safe	
http://www.founder.cj	0%	Avira URL Cloud	safe	
http://xUCQUz.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.comac	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.founder.com.cn/o	0%	Avira URL Cloud	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.urwpp.deoM	0%	Avira URL Cloud	safe	
http://www.tiro.comslnt	0%	URL Reputation	safe	
http://www.tiro.comslnt	0%	URL Reputation	safe	
http://www.tiro.comslnt	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.galapagosdesign.com/T	0%	Avira URL Cloud	safe	
http://www.sakkal.comgr	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.urwpp.deeg	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/2	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.q	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cngsP/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432748
Start date:	10.06.2021

Start time:	18:08:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	G9xXUq625O (renamed file extension from none to 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:	22
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:	mal100.troj.adwa.evad.winEXE@3/2@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.4% (good quality ratio 1.7%) • Quality average: 48.6% • Quality standard deviation: 37.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:10:13	API Interceptor	420x Sleep call for process: G9xXUq625O.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\G9xXUq625O.exe.log



Process:	C:\Users\user\Desktop\G9xXUq625O.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:ML9E4Ks29E4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MxHKX9HKx1qHiYHKhQnoPtHoxHhAHKzr
MD5:	B666A4404B132B2BF6C04FBF848EB948
SHA1:	D2EFB3D43F8B8806544D3A47F7DAEE8534981739
SHA-256:	7870616D981C8C0DE9A54E7383CD035470DB20CBF75ACDF729C32889D4B6ED96
SHA-512:	00E955EE9F14CEAE07E571A8EF2E103200CF421BAE83A66ED9F9E1AA6A9F449B653EDF1BFDB662A364D58ECF9B5FE4BB69D590DB2653F2F46A09F4D47719A862
Malicious:	true
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken= b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3 ,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Conf iguration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c56193 4e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Windows\System32\drivers\lch\hosts



Process:	C:\Users\user\Desktop\G9xXUq625O.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	11
Entropy (8bit):	2.663532754804255
Encrypted:	false
SSDEEP:	3:iLE:iLE
MD5:	B24D295C1F84ECBFB566103374FB91C5
SHA1:	6A750D3F8B45C240637332071D34B403FA1FF55A
SHA-256:	4DC7B65075FBC5B5421551F0CB814CAFDC8CACA5957D393C222EE388B6F405F4
SHA-512:	9BE279BFA70A859608B50EF5D30BF2345F334E5F433C410EA6A188DCAB395BFF50C95B165177E59A29261464871C11F903A9ECE55B2D900FE49A9F3C49EB88FA
Malicious:	true
Reputation:	high, very likely benign file
Preview:	..127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.023268235807435
TrID:	- Win32 Executable (generic) Net Framework (10011505/4) 49.83% - Win32 Executable (generic) a (10002005/4) 49.78% - Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% - Generic Win/DOS Executable (2004/3) 0.01% - DOS Executable Generic (2002/1) 0.01%
File name:	G9xXUq625O.exe
File size:	900096
MD5:	9a188a4b5ab76f5d53892f7bcd5dfbeb
SHA1:	b61e66760f0959fbb3f66daa0840eb40121827c7

General	
SHA256:	12b582ab21f7f9cd0f7475461d4f3e12ea5b8ce8ea86010e062d6dc7b5d83473
SHA512:	4c9590485c926d537e060d98c48bede5ce8cf40253ea2ea388e272a624811c7d418ba1c4e1c1f9794d25e5238a835175b705369a146e4c8ea38634680f35f82d
SSDEEP:	12288:RiqwSwbcBgHdd8+FnVQ6nGDFiDRoqlKaYdhWXUT1c9OIVfi1UarYOB79TAMHf5vW:JgQU324WFiDRoqNa7EIVfEDVB78
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$......PE..L...I.0.....@..... @.....

File Icon	
	
Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x4dc5ae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60C1986C [Thu Jun 10 04:43:24 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xda5b4	0xda600	False	0.651946864267	data	7.02711438354	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xde000	0x10f8	0x1200	False	0.377604166667	data	4.90372949588	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe0000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: G9xXUq625O.exe PID: 6320 Parent PID: 5880

General

Start time:	18:09:07
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\G9xXUq625O.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\G9xXUq625O.exe'
Imagebase:	0xe50000
File size:	900096 bytes
MD5 hash:	9A188A4B5AB76F5D53892F7BCD5DFBEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.431520750.000000000426A000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.431520750.000000000426A000.00000004.00000001.sdmp, Author: Joe Security - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.429711902.0000000003263000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: G9xXUq625O.exe PID: 7144 Parent PID: 6320

General

Start time:	18:09:52
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\G9xXUq625O.exe

Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xce0000
File size:	900096 bytes
MD5 hash:	9A188A4B5AB76F5D53892F7BCD5DFBEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.425863712.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.425863712.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.601783516.0000000003141000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.601783516.0000000003141000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.599032014.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.599032014.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis