ID: 532181
Sample Name: sKxsGhU1Wg
Cookbook: default.jbs
Time: 20:08:17
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report sKxsGhU1Wg 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: GuLoader 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
HIPS / PFW / Operating System Protection Evasion: 5
Stealing of Sensitive Information: 5
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 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 11
General 11
File Icon 12
Static PE Info 12
General 12
Entrypoint Preview 12
Rich Headers 12
Data Directories 12
Sections 12
Resources 12
Imports 12
Possible Origin 12
Network Behavior 13
Network Port Distribution 13
UDP Packets 13
DNS Queries 13
DNS Answers 13
Code Manipulations 13
Statistics 13
Behavior 13
System Behavior 13
Analysis Process: sKxsGhU1Wg.exe PID: 5356 Parent PID: 3652 13
General 13
File Activities 14
File Created 14
File Deleted 14
File Written 14

File Read 14
Analysis Process: Acly3.exe PID: 6320 Parent PID: 5356 14
General 14
File Activities 14
Analysis Process: CasPol.exe PID: 7052 Parent PID: 6320 14
General 14
File Activities 15
File Created 15
File Written 15
File Read 15
Analysis Process: conhost.exe PID: 7084 Parent PID: 7052 15
General 15
Analysis Process: misv.exe PID: 2060 Parent PID: 7052 15
General 15
File Activities 15
File Created 15
File Deleted 15
File Written 16
File Read 16
Analysis Process: misv.exe PID: 5952 Parent PID: 2060 16
General 16
File Activities 16
Disassembly 16
Code Analysis 16

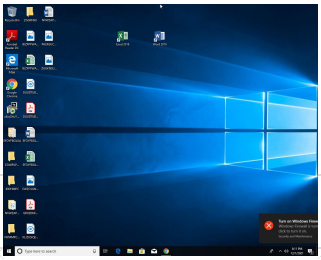
Windows Analysis Report sKxsGhU1Wg

Overview

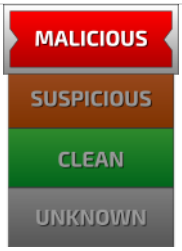
General Information

Sample Name:	sKxsGhU1Wg (renamed file extension from none to exe)
Analysis ID:	532181
MD5:	99bdb5995c8dd6..
SHA1:	7eb9e30ba8572f0.
SHA256:	c6f93eb69924750.
Tags:	32 exe
Infos:	

Most interesting Screenshot:



Detection



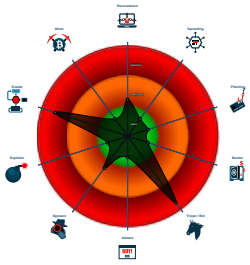
GuLoader AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- GuLoader behavior detected
- Yara detected GuLoader
- Hides threads from debuggers
- Writes to foreign memory regions
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Machine Learning detection for dropp…
- C2 URLs / IPs found in malware con…
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- sKxsGhU1Wg.exe (PID: 5356 cmdline: "C:\Users\user\Desktop\sKxsGhU1Wg.exe" MD5: 99BDB5995C8DD619A3EC2B799D1CF868)
  - Acly3.exe (PID: 6320 cmdline: C:\Users\user\AppData\Local\Temp\Acly3.exe MD5: E32061DA9B34B82E0AB5D0E53CAF5A09)
    - CasPol.exe (PID: 7052 cmdline: C:\Users\user\AppData\Local\Temp\Acly3.exe MD5: F866FC1C2E928779C7119353C3091F0C)
      - conhost.exe (PID: 7084 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - misv.exe (PID: 2060 cmdline: "C:\Users\user\AppData\Roaming\misv.exe" MD5: 1DA682EC8DCBC375B6E76660EF46D3FD)
        - misv.exe (PID: 5952 cmdline: C:\Users\user\AppData\Local\Temp\misv.exe MD5: 267CE829152E1E6B2493EE80291C3E6D)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://onedrive.live.com/download?cid=5A15FDA1AE9"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "dherdiana@rpxholding.comdha10apasmtp.rpxholding.comjo.esg2000@gmail.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.532731101.0000000003EC0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000000.422174914.000000000110 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000011.00000002.571997631.000000000368 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000007.00000002.574115115.000000001E4A 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.574115115.000000001E4A 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Click to see the 2 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect Any.run

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

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

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

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

GuLoader behavior detected

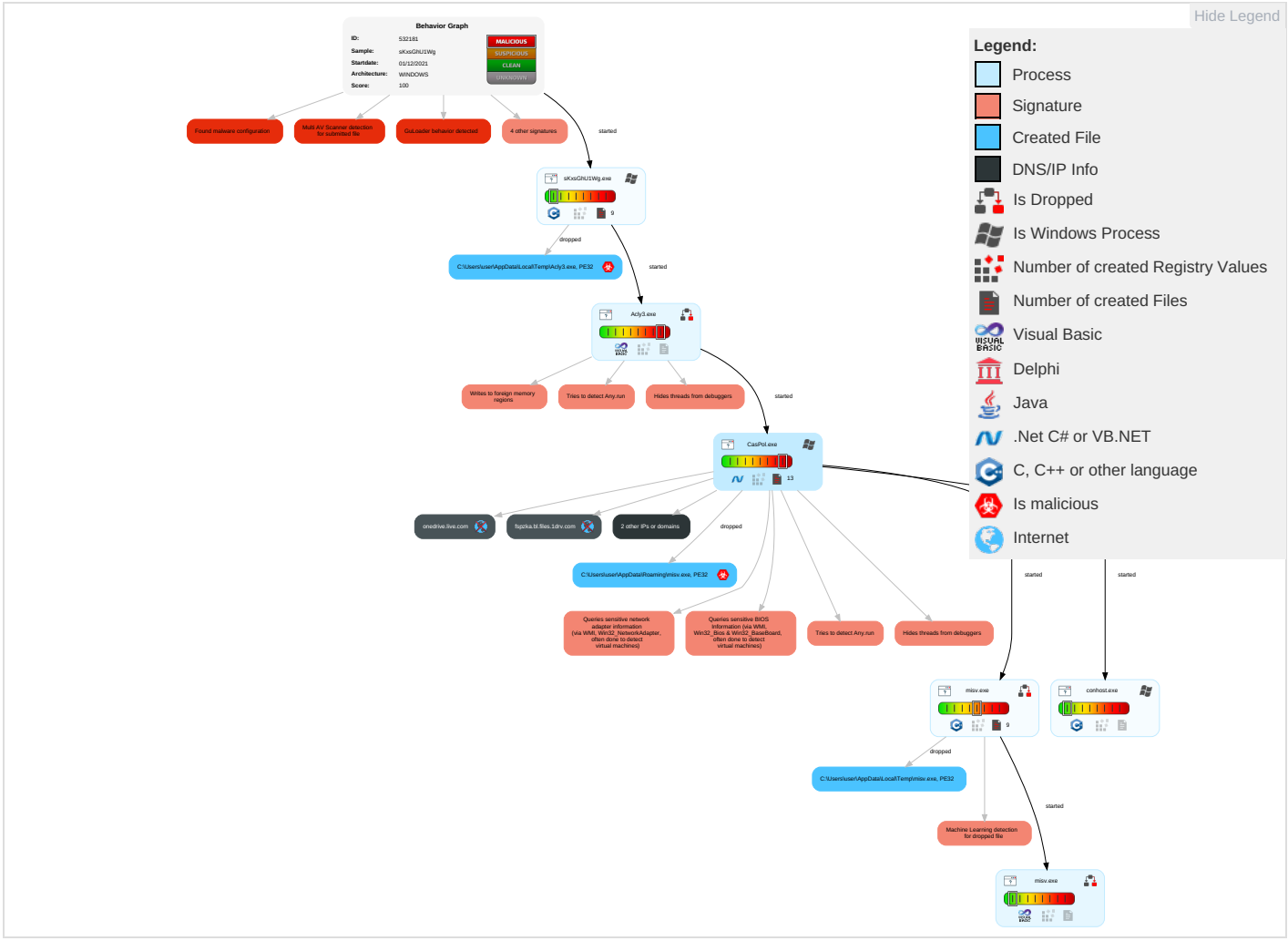
Remote Access Functionality:

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	N E
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 4 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	E I N C
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	E F C
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 1	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	N D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 1 6	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	F A

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
sKxsGhU1Wg.exe	11%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\misv.exe	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://rOTpQz.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
onedrive.live.com	unknown	unknown	false		high
eruitg.bl.files.1drv.com	unknown	unknown	false		high
fspzka.bl.files.1drv.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/download?cid=5A15FDA1AE9	false		high

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532181
Start date:	01.12.2021
Start time:	20:08:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sKxsGhU1Wg (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:	21
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.evad.winEXE@10/3@3/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 97.1%) • Quality average: 84.4% • Quality standard deviation: 23.8%
HCA Information:	• Successful, ratio: 71% • 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
20:11:23	API Interceptor	14x Sleep call for process: CasPol.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\Acly3.exe

Process:	C:\Users\user\Desktop\sKxsGhU1Wg.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	21304624
Entropy (8bit):	0.09518636040127255
Encrypted:	false
SSDEEP:	1536:j30RIkuZxe033g6Oixa+IC8KNXA/wMy2dWVu2h55nw6+717EQZ4yr3hShX:j30qHZxT3gsxaZmNXYy7zysx
MD5:	E32061DA9B34B82E0AB5D0E53CAF5A09
SHA1:	5AABAD649F6C4B826C30BDF8152E6F8D33CB8133
SHA-256:	7C9AEB4763912BE27C0B5CFE843642E4424902DD2EEFB1AD2DF6092EBF10A468
SHA-512:	EBF93E81A0AB530EA19131F490A2423E017384357731FBE5CAC4D60876C5B535E371BB9443D62AEA8F41D732079EAB2A6EDD4335EDEAAD086EED2410D5914F54
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,..SM.SM.SM..Q..RM..o.UM.ek.RM.RichSM.....PE..L.. ..#L.....B.....$..... ....@.....E.....QE.....t...(....0....B.....P.E.....0... .....text...$. ....`.data...p.... ....@....rsrc.....B..0....B..0.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Temp\misv.exe	
Process:	C:\Users\user\AppData\Roaming\misv.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	21214512
Entropy (8bit):	0.09651890759201205
Encrypted:	false
SSDEEP:	1536:eMFtMi1UWzCVv7k95bpw45zcJHJEWR4kpDatDwlvpa7WA/xJ2gaQsv6hWfl3hR2S:1jMCUWUv7k95Vw4pupzRrNAFl+2S
MD5:	267CE829152E1E6B2493EE80291C3E6D
SHA1:	814FEDAD9318740DC21569DA4B900AC9A2CE1270
SHA-256:	25526139AACB45F3F8C4F5A6623CA50635163E882F922B908F5A3BF3A94D42EE
SHA-512:	3CF20247D421E04D6D154B7C5F8B31943A4DA6FF7EF677A9DD290AF745AD89F802209D6FFD4C573B02186CEDDCB73784E772FA9599A6C88CD2D05C0656A005(
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,..SM.SM.SM..Q..RM..o.UM.ek.RM.RichSM.....PE..L.. ../.I.....A.....$..... ....@.....C.....C.....(....0..plA.....P.C.....0.. .....text..... ....`.data...p.... ....@....rsrc...plA..0...pA..0.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Roaming\misv.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	135018
Entropy (8bit):	7.060957913639306
Encrypted:	false
SSDEEP:	3072:gbG7N2kDTHUpou4ubvh1q2SRdteVQNOqeOEgyVlzba:gbE/HUjva2udnNOqbByVlPa
MD5:	1DA682EC8DCBC375B6E76660EF46D3FD
SHA1:	B7DA4D771226B5A4F045B0D8A263451612EE3303
SHA-256:	6D624544826CC99182030BB50757944FEE3734EA01E8C37A77A22214BFF4B9DF
SHA-512:	2077475610EAA19020D7AFA36896B3E995D66651F4D0E8B4EB8523D64EA8C4B5C48778081182C033FD3C330A253EF8FA34E935BAD4EF7947CD17EE09B126AA4
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
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.....-5.....@.....@..... .....text....h.....j..... ..`.rdata.....n.....@..@.data.....@....ndata...`...`.....rsrc.....@..@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.073841941088541
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:	sKxsGhU1Wg.exe
File size:	131595
MD5:	99bdb5995c8dd619a3ec2b799d1cf868
SHA1:	7eb9e30ba8572f07a1e88972ad8f14954e84eb39
SHA256:	c6f93eb69924750adbe61115b2d6a200d534e783c6bd4ca0e2c0cd2969e9469e
SHA512:	8a2817d4cd4d9584c0c723ca96550b65f530c6de6193b977239ce3c90c8eb0e3942b7ecf2ac3f12c730ae053c3a88993d54bfed16fee6b2cc5aa5083105c52d6
SSDEEP:	3072:gbG7N2kDTHUpou4ub+HbksLwq6cttYgSj+LaQitS42:gbE/HUjwkshtOlj+LaQitE

General

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:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40352d
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	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

Entrypoint Preview

Rich Headers

Data Directories

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	0x16000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x4c000	0x11e0	0x1200	False	0.368489583333	data	4.48173978815	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 1, 2021 20:11:01.993771076 CET	192.168.2.3	8.8.8.8	0x2e78	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Dec 1, 2021 20:11:02.738807917 CET	192.168.2.3	8.8.8.8	0x3585	Standard query (0)	eruitg.bl.files.1drv.com	A (IP address)	IN (0x0001)
Dec 1, 2021 20:11:05.786591053 CET	192.168.2.3	8.8.8.8	0x9dc6	Standard query (0)	fspzka.bl.files.1drv.com	A (IP address)	IN (0x0001)

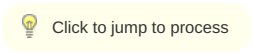
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 1, 2021 20:11:02.021389008 CET	8.8.8.8	192.168.2.3	0x2e78	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 20:11:02.851330042 CET	8.8.8.8	192.168.2.3	0x3585	No error (0)	eruitg.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 20:11:02.851330042 CET	8.8.8.8	192.168.2.3	0x3585	No error (0)	bl-files.fe.1drv.com	odc-bl-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 20:11:05.829888105 CET	8.8.8.8	192.168.2.3	0x9dc6	No error (0)	fspzka.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 20:11:05.829888105 CET	8.8.8.8	192.168.2.3	0x9dc6	No error (0)	bl-files.fe.1drv.com	odc-bl-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: sKxsGhU1Wg.exe PID: 5356 Parent PID: 3652

General

Start time:	20:09:19
Start date:	01/12/2021
Path:	C:\Users\user\Desktop\sKxsGhU1Wg.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\sKxsGhU1Wg.exe"
Imagebase:	0x400000
File size:	131595 bytes
MD5 hash:	99BDB5995C8DD619A3EC2B799D1CF868
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: Acly3.exe PID: 6320 Parent PID: 5356

General

Start time:	20:09:21
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Local\Temp\Acly3.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Acly3.exe
Imagebase:	0x400000
File size:	21304624 bytes
MD5 hash:	E32061DA9B34B82E0AB5D0E53CAF5A09
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.532731101.0000000003EC0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: CasPol.exe PID: 7052 Parent PID: 6320

General

Start time:	20:10:15
Start date:	01/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Acly3.exe
Imagebase:	0xcf0000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000007.00000000.422174914.0000000001100000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.574115115.000000001E4A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.574115115.000000001E4A1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 7084 Parent PID: 7052

General

Start time:	20:10:17
Start date:	01/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: misv.exe PID: 2060 Parent PID: 7052

General

Start time:	20:11:03
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Roaming\misv.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\misv.exe"
Imagebase:	0x400000
File size:	135018 bytes
MD5 hash:	1DA682EC8DCBC375B6E76660EF46D3FD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: misv.exe PID: 5952 Parent PID: 2060

General

Start time:	20:11:07
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Local\Temp\misv.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\misv.exe
Imagebase:	0x400000
File size:	21214512 bytes
MD5 hash:	267CE829152E1E6B2493EE80291C3E6D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000011.00000002.571997631.0000000003680000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Disassembly

Code Analysis