ID: 546024
Sample Name: awxVepPEpA
Cookbook: default.jbs
Time: 20:07:09
Date: 28/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

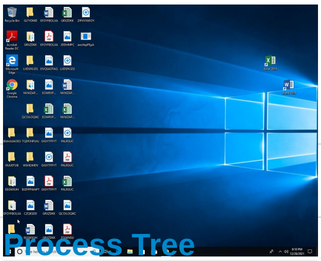
Windows Analysis Report awxVepPEpA

Overview

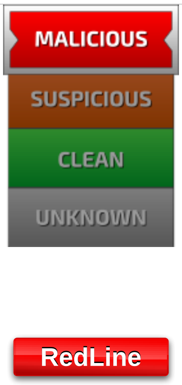
General Information

Sample Name:	awxVepPEpA (renamed file extension from none to exe)
Analysis ID:	546024
MD5:	110526d2882da3..
SHA1:	250a483cead19e..
SHA256:	772f0c407388e02.
Tags:	32 exe RedLineStealer trojan
Infos:	

Most interesting Screenshot:



Detection

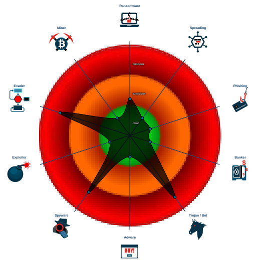


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Found malware configuration
- Multi AV Scanner detection for subm…
- Writes to foreign memory regions
- Tries to shutdown other security too…
- Tries to steal Crypto Currency Wallets
- Connects to many ports of the same…
- Machine Learning detection for samp…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- Queries sensitive video device inform…
- PE file has nameless sections

Classification



Process Tree

- **System is w10x64**
- awxVepPEpA.exe (PID: 3084 cmdline: "C:\Users\user\Desktop\awxVepPEpA.exe" MD5: 110526D2882DA3D46AA3D7023B00F41E)
  - AppLaunch.exe (PID: 1008 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
- **cleanup**

Malware Configuration

Threatname: RedLine

```
{
  "C2 url": "85.209.89.134:41320",
  "Bot Id": "@flop_tc"
}
```

Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.231691926.00000000000C2000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000003.00000002.287138246.0000000000402000.00000020.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000003.231382400.0000000003722000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.289189345.0000000007249000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: AppLaunch.exe PID: 1008	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.AppLaunch.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.3.awxVepPEpA.exe.3720000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.awxVepPEpA.exe.c3aec.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.awxVepPEpA.exe.c3aec.0.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

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 sample

Networking:

Connects to many ports of the same IP (likely port scanning)

System Summary:

PE file has nameless sections

Malware Analysis System Evasion:

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Tries to shutdown other security tools via broadcasted WM_QUERYENDSESSION

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

Found many strings related to Crypto-Wallets (likely being stolen)

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

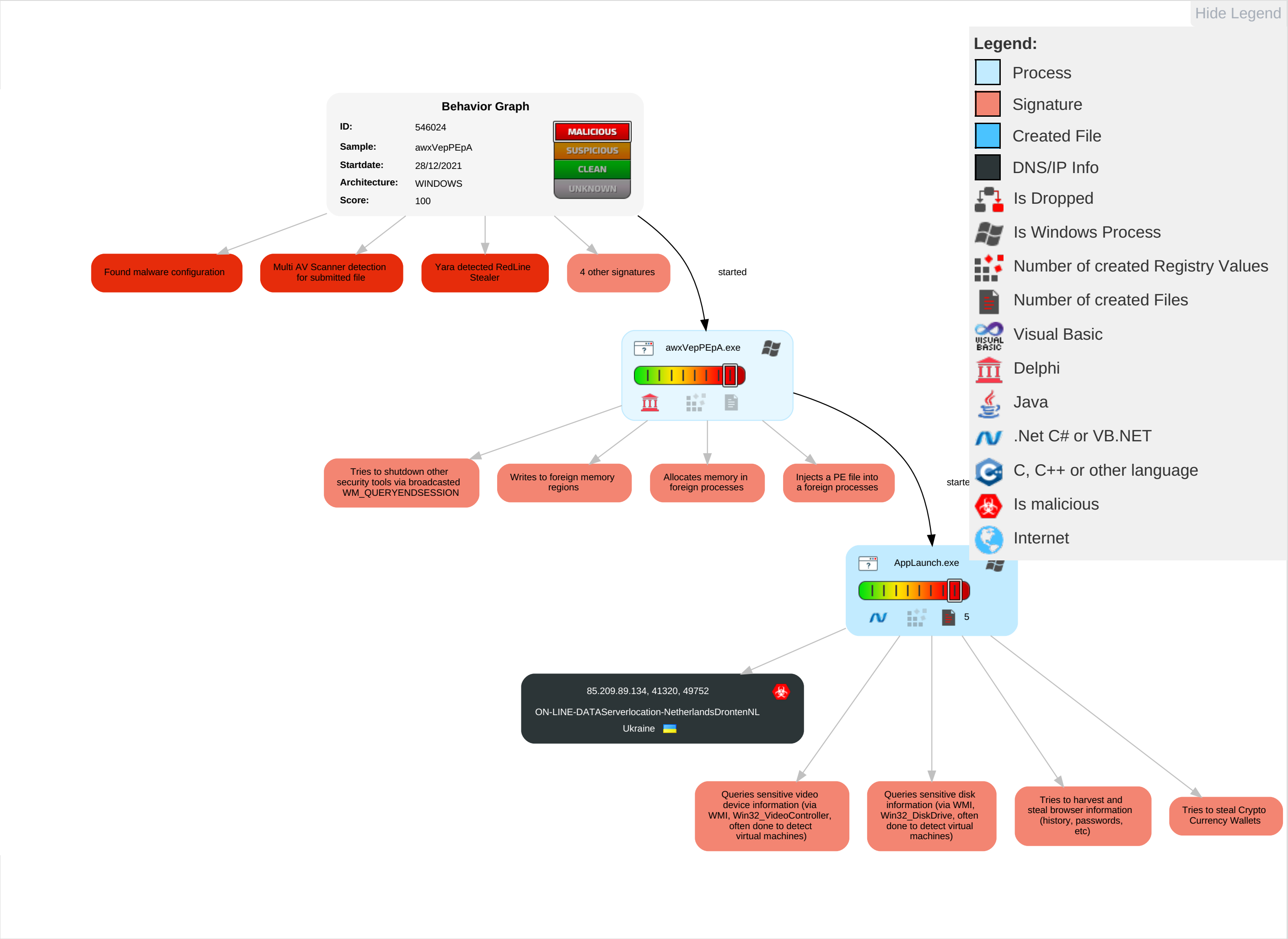
Remote Access Functionality:

Yara detected RedLine Stealer

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

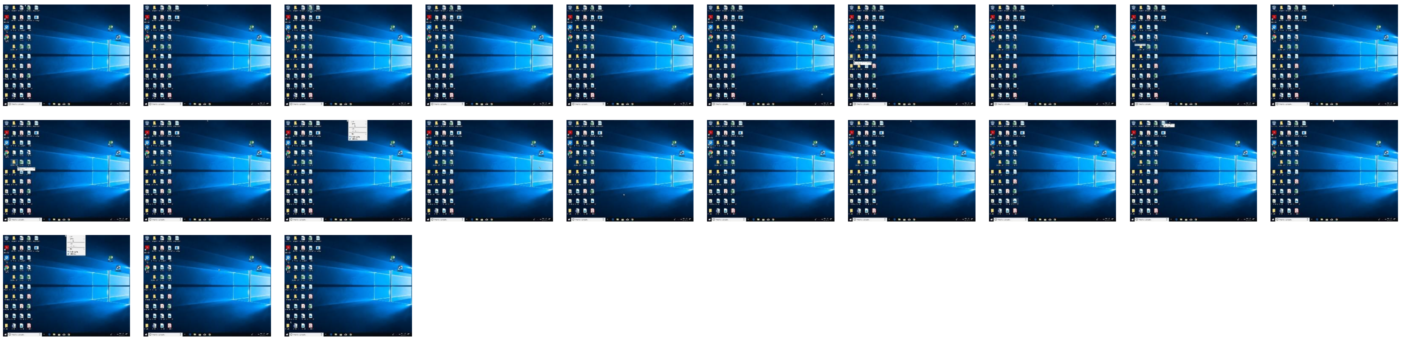
Behavior Graph

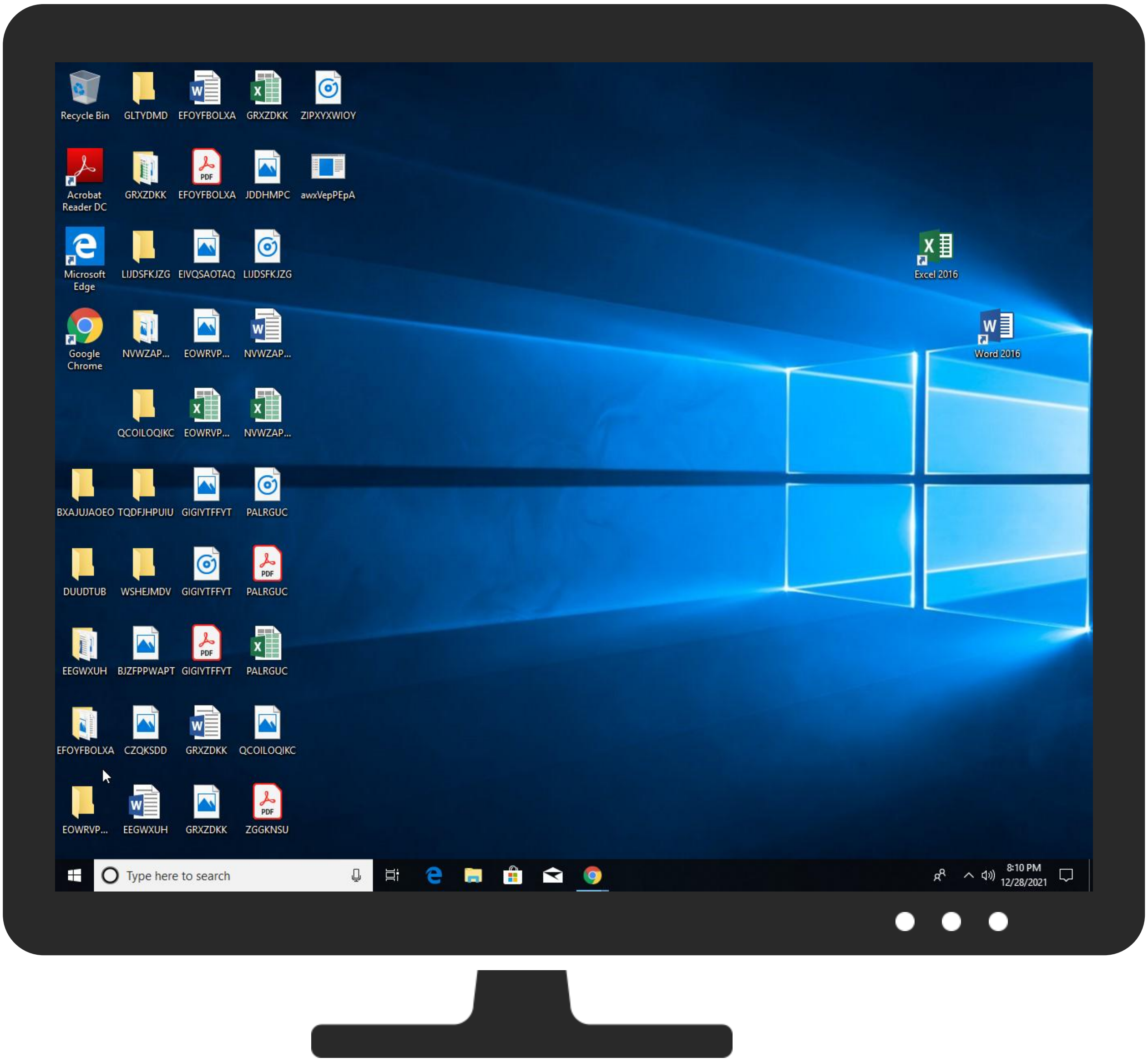

Hide Legend
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet
Behavior Graph
ID: 546024
Sample: awxVepPEpA
Startdate: 28/12/2021
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Found malware configuration
Multi AV Scanner detection for submitted file
Yara detected RedLine Stealer
4 other signatures
started
awxVepPEpA.exe
Tries to shutdown other security tools via broadcasted WM_QUERYENDSESSION
Writes to foreign memory regions
Allocates memory in foreign processes
Injects a PE file into a foreign processes
starte
AppLaunch.exe
5
85.209.89.134, 41320, 49752
ON-LINE-DATAServerlocation-NetherlandsDrontenNL
Ukraine
Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)
Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)
Tries to harvest and steal browser information (history, passwords, etc)
Tries to steal Crypto Currency Wallets

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
awxVepPEpA.exe	54%	Virustotal		Browse
awxVepPEpA.exe	23%	Metadefender		Browse
awxVepPEpA.exe	51%	ReversingLabs	Win32.Infostealer.Convagent	
awxVepPEpA.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.awxVepPEpA.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.awxVepPEpA.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.1.awxVepPEpA.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://iptc.tc4xmp	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23Response	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.209.89.134	unknown	Ukraine	🇺🇦	204601	ON-LINE-DATAServerlocation-NetherlandsDrontenNL	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	546024
Start date:	28.12.2021
Start time:	20:07:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	awxVepPEpA (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:	24
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.spyw.evad.winEXE@3/1@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.9% (good quality ratio 1.5%) • Quality average: 57.3% • Quality standard deviation: 40.5%
HCA Information:	• Successful, ratio: 70% • 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
20:08:22	API Interceptor	35x Sleep call for process: AppLaunch.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\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MOfHK5HKXAHKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHKAHK1HxLHG1qHqH5HX:vq5qXAqLqdqUqzcGYqhQnoPtIxHbqAqG
MD5:	174E563C986AB09114A6F31F870A6E13
SHA1:	F68EFDC04D0559B24C448E629A0115F2E6C3B39D
SHA-256:	465C8001CEFD747AF8A94EDD62CC829D8DFF4D6BED174591DA0B71E10FDC584F
SHA-512:	252A2B615BB7BB4223F0873F41CC7C4BC6576172CD704DD93926E004CD5795CA5DC2DE3332586BF3C44E0B564148A7661563C00B204649C7A5594C097C1E9EC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.ServiceModel.Internals, Version=4.0.0.0, Culture=

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.998681450351388
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Win16/32 Executable Delphi generic (2074/23) 0.02% • 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:	awxVepPEpA.exe
File size:	3617280
MD5:	110526d2882da3d46aa3d7023b00f41e
SHA1:	250a483cead19e65bc11d215d48289dff51241b0
SHA256:	772f0c407388e029e98f9d885f57a0e3ef9b0f42099a16fe6367fb321d4e2444
SHA512:	46b4bd385342adcbbf52037d8c6b68609aed852dafde949 022715f40f18af30f31497f30f49cdc1d0d9cb98a569d8b9 3079288b0b1926414413a0c20074ad6c6
SSDEEP:	98304:4/lpBz0Mi19cNcuurKu0stiPJajebo04XY4OiCKU:4/lEz9cNnuRDOKio04vOiCR
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.......a................. ....@....@..........................0U.......7....................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x401000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x61C6DCEB [Sat Dec 25 08:57:15 2021 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:	c284fa365c4442728ac859c0f9ed4dc5

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
	0x1000	0x22000	0x11200	False	1.00044194799	data	7.99711453077	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x23000	0x47c	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x24000	0xf000	0x7800	False	1.00052083333	data	7.9942215702	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x33000	0x2000	0x400	False	1.0107421875	data	7.79345594108	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x35000	0x1888fe	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x1be000	0x32b000	0x2f9c00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x4e9000	0x3000	0x1a00	False	1.00165264423	data	7.97396561553	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x4ec000	0x1b000	0x13a00	False	0.999701433121	data	7.99695916307	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tZjoKcx	0x507000	0x4b000	0x4b000	False	0.987112630208	data	7.91909215806	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.adata	0x552000	0x1000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: awxVepPEpA.exe PID: 3084 Parent PID: 5176

General

Start time:	20:07:59
Start date:	28/12/2021
Path:	C:\Users\user\Desktop\awxVepPEpA.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\awxVepPEpA.exe"
Imagebase:	0x400000
File size:	3617280 bytes
MD5 hash:	110526D2882DA3D46AA3D7023B00F41E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.231691926.00000000000C2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.231382400.0000000003722000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: AppLaunch.exe PID: 1008 Parent PID: 3084

General

Start time:	20:08:00
Start date:	28/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0x13d0000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000003.00000002.287138246.0000000000402000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.289189345.0000000007249000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 34.0.0 Boulder Opal