ID: 323615
Sample Name: AWB-18267638920511_ES.exe
Cookbook: default.jbs
Time: 08:29:16
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

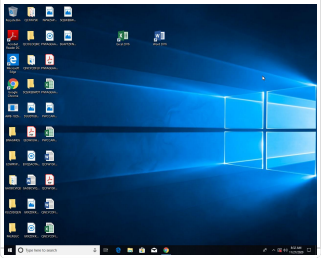
Analysis Report AWB-18267638920511_ES.exe

Overview

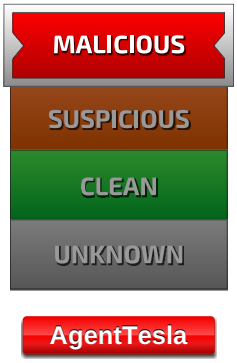
General Information

Sample Name:	AWB-18267638920511_ES.exe
Analysis ID:	323615
MD5:	8b7f30a440fcc0b..
SHA1:	b3c91697ef02a5d.
SHA256:	b437404019d387..
Tags:	AgentTesla

Most interesting Screenshot:



Detection

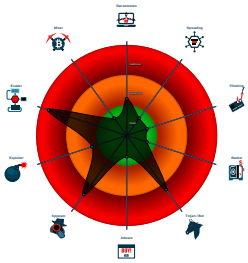


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …

Classification



Startup

- **System is w10x64**
- AWB-18267638920511_ES.exe (PID: 3984 cmdline: 'C:\Users\user\Desktop\AWB-18267638920511_ES.exe' MD5: 8B7F30A440FCC0B4B4EA690ECBFFF43E)
  - schtasks.exe (PID: 5944 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\tGjZeZC' /XML 'C:\Users\user\AppData\Local\Temp\tmpA7E.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6140 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AWB-18267638920511_ES.exe (PID: 3728 cmdline: {path} MD5: 8B7F30A440FCC0B4B4EA690ECBFFF43E)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "RrY9j3ju7QQ",
  "URL: ": "http://51Rg6ceg1VdsK.net",
  "To: ": "winwinner151@gmail.com",
  "ByHost: ": "mail.talleresgenerauto.es:587",
  "Password: ": "S2vtG9cNKv",
  "From: ": "chapaypintura@talleresgenerauto.es"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.470115094.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.474541903.0000000002DF1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.474541903.0000000002DF1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.223775772.00000000042A4000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.475012814.0000000002EA4000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 7 entries				

Unpacked PEs

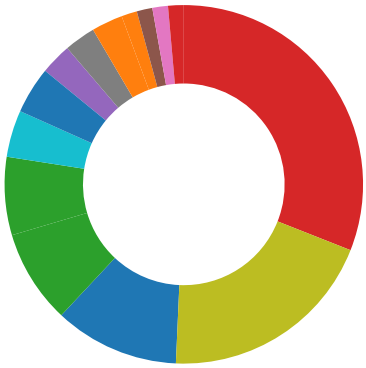
Source	Rule	Description	Author	Strings
3.2.AWB-18267638920511_ES.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



Click to jump to signature section

- AV Detection
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

System Summary:

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

- Yara detected AntiVM_3
- 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)
- Queries sensitive video device information (via WMI, Win32_VideoController, 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

Stealing of Sensitive Information:

- Yara detected AgentTesla
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
- Tries to harvest and steal browser information (history, passwords, etc)
- Tries to harvest and steal ftp login credentials
- Tries to steal Mail credentials (via file access)

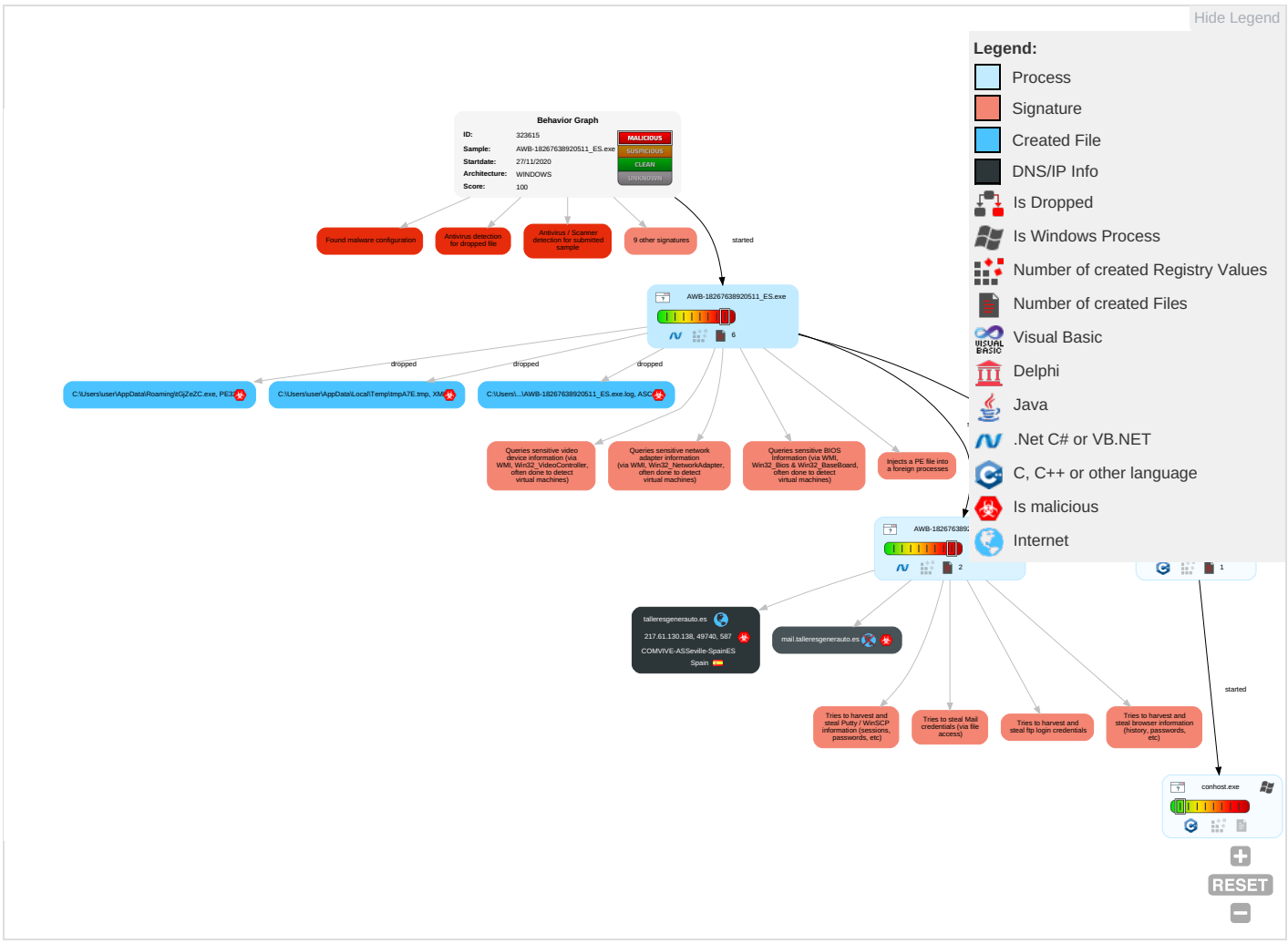
Remote Access Functionality:

- 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
Valid Accounts	Windows Management Instrumentation 3 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 2 4	Credentials in Registry 1	Security Software Discovery 4 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)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 2 4	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	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 3	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	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	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 1 4	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
AWB-18267638920511_ES.exe	76%	ReversingLabs	ByteCode-MSIL.Infostealer.Stelega	
AWB-18267638920511_ES.exe	100%	Avira	TR/AD.AgentTesla.bldep	
AWB-18267638920511_ES.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\tGjZeZC.exe	100%	Avira	TR/AD.AgentTesla.bldep	
C:\Users\user\AppData\Roaming\tGjZeZC.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\tGjZeZC.exe	76%	ReversingLabs	ByteCode-MSIL.Infostealer.Stelega	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.AWB-18267638920511_ES.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

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	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	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://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://LVvtpY.com	0%	Avira URL Cloud	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.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://talleresgenerauto.es	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://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	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://51Rg6ceg1VdsK.net	0%	Avira URL Cloud	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.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.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.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://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.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://mail.talleresgenerauto.es	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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	
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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
talleresgenerauto.es	217.61.130.138	true	true		unknown
mail.talleresgenerauto.es	unknown	unknown	true		unknown

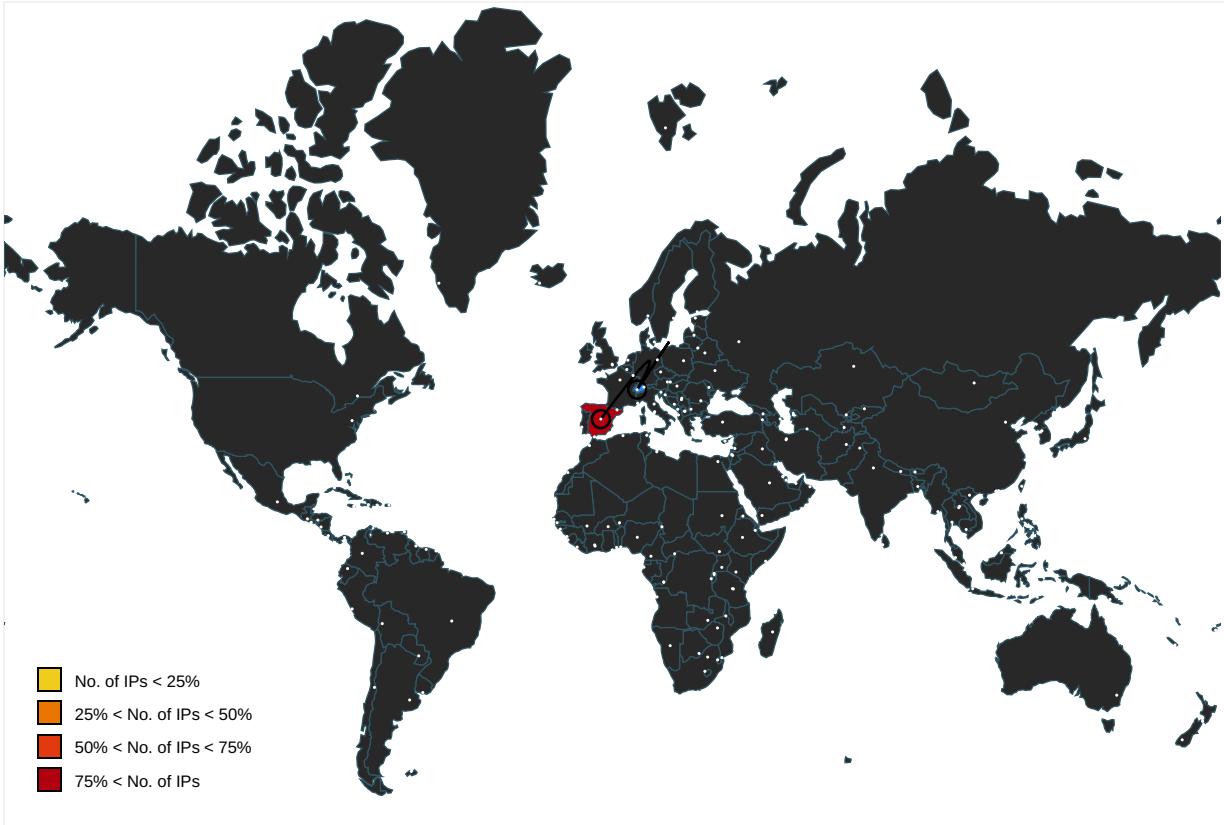
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	AWB-18267638920511_ES.exe, 00000003.00000002.474541903.00000002DF1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	AWB-18267638920511_ES.exe, 00000003.00000002.474541903.00000002DF1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	AWB-18267638920511_ES.exe, 00000003.00000002.480483982.000067F0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	AWB-18267638920511_ES.exe, 00000003.00000002.474541903.00000002DF1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://LVvtpY.com	AWB-18267638920511_ES.exe, 00000003.00000002.474541903.00000002DF1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false		high
http://www.tiro.com	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.goodfont.co.kr	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://talleresgenerauto.es	AWB-18267638920511_ES.exe, 00000003.00000002.475508407.0000000002F30000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	AWB-18267638920511_ES.exe, 00000003.00000002.474541903.0000000002DF1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://51Rg6ceg1VdsK.net	AWB-18267638920511_ES.exe, 00000003.00000002.475012814.0000000002EA4000.00000004.00000001.sdmp, AWB-18267638920511_ES.exe, 00000003.00000002.475259720.0000000002EFB000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.typography.netD	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/	AWB-18267638920511_ES.exe, 00000000.00000002.223775772.000000042A4000.00000004.00000001.sdmp, AWB-18267638920511_ES.exe, 00000003.00000002.470115094.0000000000402000.00000040.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false		high
http://www.fonts.com	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.talleresgenerauto.es	AWB-18267638920511_ES.exe, 00000003.00000002.475508407.0000000002F30000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	AWB-18267638920511_ES.exe, 00000000.00000002.223047556.0000000003201000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	AWB-18267638920511_ES.exe, 00000000.00000002.227857134.00000000072C2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	AWB-18267638920511_ES.exe, 00000003.00000002.474541903.00000002DF1000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	AWB-18267638920511_ES.exe, 00000000.00000002.223775772.000000042A4000.00000004.00000001.sdmp, AWB-18267638920511_ES.exe, 00000003.00000002.470115094.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
217.61.130.138	unknown	Spain		39020	COMVIVE-ASSeville-SpainES	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323615
Start date:	27.11.2020
Start time:	08:29:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AWB-18267638920511_ES.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:	23
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@6/3@2/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 52.147.198.201, 104.43.139.144, 51.104.139.180, 92.122.144.200, 20.54.26.129, 205.185.216.10, 205.185.216.42, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/323615/sample/AWB-18267638920511_ES.exe

Simulations

Behavior and APIs

Time	Type	Description
08:30:09	API Interceptor	789x Sleep call for process: AWB-18267638920511_ES.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
COMVIVE-ASSeville-SpainES	cUnk2St74R.exe	Get hash	malicious	Browse	• 217.61.130.106
	8UZQ3kv5fg.exe	Get hash	malicious	Browse	• 217.61.130.106
	http://8068e-4812f.preview.sitejet.io/	Get hash	malicious	Browse	• 217.61.130.111
	http://https://niw.academy/New/DocSigning.htm	Get hash	malicious	Browse	• 185.50.196.212
	ATTACHMENT_092020_818717005.doc	Get hash	malicious	Browse	• 185.50.196.212
	DOC-9576850.doc	Get hash	malicious	Browse	• 217.61.130.34
	Soumissions 893963.doc	Get hash	malicious	Browse	• 217.61.130.34
	http://https://1349fk.com/admin/55rEgXThCrasXK9fnSP	Get hash	malicious	Browse	• 217.61.130.34
	http://localesfavoritos.com/wp-admin/Document/	Get hash	malicious	Browse	• 217.61.130.34
	http://https://portondeguadarrama.com/jss/OD	Get hash	malicious	Browse	• 217.61.130.111
	script.exe.7582a080.0x0000000002360000-0x0000000002401fff.exe	Get hash	malicious	Browse	• 185.50.197.168
	SOC report 07 22 2020.doc	Get hash	malicious	Browse	• 185.50.196.201
	Form - Jul 22, 2020.doc	Get hash	malicious	Browse	• 185.50.196.201
	Form - Jul 22, 2020.doc	Get hash	malicious	Browse	• 185.50.196.201
	http://https://tutoriapro.com/storage/FILE/2f1rhht/	Get hash	malicious	Browse	• 185.50.196.201
	http://https://contabilidaddecostes.com/todwll/?email=cynthia.hng@vodafone.com	Get hash	malicious	Browse	• 185.50.199.194

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AWB-18267638920511_ES.exe.log

Process:	C:\Users\user\Desktop\AWB-18267638920511_ES.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1393
Entropy (8bit):	5.336387678668898
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AWB-18267638920511_ES.exe.log	
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4VE4x84F0:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz4
MD5:	918F04BB59A8331CBEAD9305F6A98022
SHA1:	DC143AF1885A9FD5964AE0CD2C0C9248459D69FA
SHA-256:	89CAD35E7AB95E575A209A676E91D005B1E1342D172F9559CA47D9617A9DE6DB
SHA-512:	B31C671F3CAAE013679DF07D191AAC2902EC052313601715C1FA44D63925931F610089E02E5D405A5ED337809ED227B5C0A2B88C9F06234DA4EBA27B1446DD7A
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, 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,"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\f1d8480152e0da9a60ad49c6d16a3b6d\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.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.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\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmpA7E.tmp	
Process:	C:\Users\user\Desktop\AWB-18267638920511_ES.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1640
Entropy (8bit):	5.192867902772148
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKBDCtn:cbh47TlNQ//rydbz9l3YODOLNdq3xk
MD5:	AD32B7CBBF8CF25C353C52DDBC4ED48D
SHA1:	E5AA7D62DD5DE428785FBB74D993FAEB4346C67A
SHA-256:	3B4550E354423B8A098BCC6BA56FDB91825850BBE4B05809A9E56C386858F1C7
SHA-512:	A54D15894E3E82E6FF28D836FE953047E841DE287EA3B6C8B5907AF100C4EB9DA22D3E6E0309B1BB19FA87FBBAB5946AD395469409A5C8D7FCA2703BC2E9B4CF
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\tGjZeZC.exe	
Process:	C:\Users\user\Desktop\AWB-18267638920511_ES.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	531456
Entropy (8bit):	7.6437799109521265
Encrypted:	false
SSDEEP:	12288:LfA7j4whhjZADjbOlv611wmRDa+Ze9jKxnnUOvYCGb7aOt8LFXDQI5jwmGfTgm:Lf4hjZUj0vzMDadmxn9vYLbB8Nk
MD5:	8B7F30A440FCC0B4B4EA690ECBFFF43E
SHA1:	B3C91697EF02A5D357849E6358D825FDAB37A69E
SHA-256:	B437404019D38740807EE024FCE54AC262690C6BCC59E893B7D8CA4392E7465A
SHA-512:	EAA52E8F3AF0F95B9E3AA54A4F4BBD259F926C400748A5F013EC24A51C3246911BF21DA46C3EC3BDDF42D45BBA382DFEA2052BF43BE94CA88A752D7E6BD3B41C
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 76%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...g..._.....>0... ...@....@.. .....@.....@...../..W....@.....`..... ..... ..H.....text...D.... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B..... 0.....H.....P....5.....X`.....*".(.....*Vr...p.....r...p.....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*>...(g...(.....*:..(....(i....*...(....(T...(!...(U.....(.....(A....*...(.....{C....(&.....(....o$.....{....(m....*....(.....(.....(.....{$....(.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.6437799109521265
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.98% • Win32 Executable (generic) a (10002005/4) 49.93% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	AWB-18267638920511_ES.exe
File size:	531456
MD5:	8b7f30a440fcc0b4b4ea690ecbfff43e
SHA1:	b3c91697ef02a5d357849e6358d825fdab37a69e
SHA256:	b437404019d38740807ee024fce54ac262690c6bcc59e893b7d8ca4392e7465a
SHA512:	eaa52e8f3af0f95b9e3aa54a4f4bbd259f926c400748a5f013ec24a51c3246911bf21da46c3ec3bddf42d45bba382dfea2052bf43be94ca88a752d7e6bd3b41c
SSDEEP:	12288:LfA7j4whhjZADjbOlv611wmRDa+Ze9jKxnnUOvYCGb7aOt8LFXDQI5jwmGfTgm:Lf4hjZUj0vzMDadmxn9vYLbB8Nk
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...g..._.....>0... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x48303e
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:	0x5FBE0767 [Wed Nov 25 07:27:35 2020 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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x82fe4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x84000	0x590	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x86000	0xc	.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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x81044	0x81200	False	0.78805474044	data	7.65240635484	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x84000	0x590	0x600	False	0.414713541667	data	4.03754982361	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x86000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x840a0	0x304	data		
RT_MANIFEST	0x843a4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

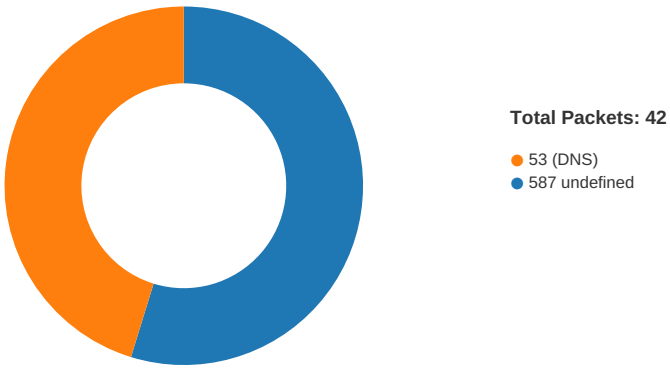
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2019
Assembly Version	1.0.0.0
InternalName	I.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	SnakeGame
ProductVersion	1.0.0.0
FileDescription	SnakeGame
OriginalFilename	I.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 08:31:51.072638988 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:51.125221014 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:51.125420094 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:51.319319963 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:51.319869041 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:51.372632027 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:51.373213053 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:51.430037022 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:51.483082056 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:51.505405903 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:51.598007917 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:51.604352951 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:51.604420900 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:51.604475021 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:51.604501963 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:51.604682922 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:51.604738951 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:51.606837034 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:51.654958963 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:51.658413887 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:51.710905075 CET	587	49740	217.61.130.138	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 08:31:51.711494923 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:51.764344931 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:51.972313881 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:52.025181055 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:52.027930975 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:52.083364964 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:52.084773064 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:52.145201921 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:52.146691084 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:52.199361086 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:52.199779034 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:52.292516947 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:52.300750971 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:52.301438093 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:52.353976011 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:52.355387926 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:52.355523109 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:52.356446981 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:52.357044935 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:31:52.407833099 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:52.407855988 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:52.408795118 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:52.409231901 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:52.417999029 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:31:52.467456102 CET	49740	587	192.168.2.3	217.61.130.138
Nov 27, 2020 08:32:07.520045042 CET	587	49740	217.61.130.138	192.168.2.3
Nov 27, 2020 08:32:07.520199060 CET	49740	587	192.168.2.3	217.61.130.138

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 08:30:00.449664116 CET	60100	53	192.168.2.3	8.8.8.8
Nov 27, 2020 08:30:00.485167027 CET	53	60100	8.8.8.8	192.168.2.3
Nov 27, 2020 08:30:01.289424896 CET	53195	53	192.168.2.3	8.8.8.8
Nov 27, 2020 08:30:01.324779987 CET	53	53195	8.8.8.8	192.168.2.3
Nov 27, 2020 08:30:01.946873903 CET	50141	53	192.168.2.3	8.8.8.8
Nov 27, 2020 08:30:01.982410908 CET	53	50141	8.8.8.8	192.168.2.3
Nov 27, 2020 08:30:02.913254976 CET	53023	53	192.168.2.3	8.8.8.8
Nov 27, 2020 08:30:02.940493107 CET	53	53023	8.8.8.8	192.168.2.3
Nov 27, 2020 08:30:03.732403994 CET	49563	53	192.168.2.3	8.8.8.8
Nov 27, 2020 08:30:03.767829895 CET	53	49563	8.8.8.8	192.168.2.3
Nov 27, 2020 08:30:04.507401943 CET	51352	53	192.168.2.3	8.8.8.8
Nov 27, 2020 08:30:04.534513950 CET	53	51352	8.8.8.8	192.168.2.3
Nov 27, 2020 08:30:06.451210022 CET	59349	53	192.168.2.3	8.8.8.8
Nov 27, 2020 08:30:06.478133917 CET	53	59349	8.8.8.8	192.168.2.3
Nov 27, 2020 08:30:07.156336069 CET	57084	53	192.168.2.3	8.8.8.8
Nov 27, 2020 08:30:07.183568001 CET	53	57084	8.8.8.8	192.168.2.3
Nov 27, 2020 08:30:07.821103096 CET	58823	53	192.168.2.3	8.8.8.8
Nov 27, 2020 08:30:07.848185062 CET	53	58823	8.8.8.8	192.168.2.3
Nov 27, 2020 08:30:29.337064981 CET	57568	53	192.168.2.3	8.8.8.8
Nov 27, 2020 08:30:29.364278078 CET	53	57568	8.8.8.8	192.168.2.3
Nov 27, 2020 08:30:32.922466040 CET	50540	53	192.168.2.3	8.8.8.8
Nov 27, 2020 08:30:32.959696054 CET	53	50540	8.8.8.8	192.168.2.3
Nov 27, 2020 08:30:46.489939928 CET	54366	53	192.168.2.3	8.8.8.8
Nov 27, 2020 08:30:46.542834044 CET	53	54366	8.8.8.8	192.168.2.3
Nov 27, 2020 08:30:49.497139931 CET	53034	53	192.168.2.3	8.8.8.8
Nov 27, 2020 08:30:49.524254084 CET	53	53034	8.8.8.8	192.168.2.3
Nov 27, 2020 08:31:03.385047913 CET	57762	53	192.168.2.3	8.8.8.8
Nov 27, 2020 08:31:03.412233114 CET	53	57762	8.8.8.8	192.168.2.3
Nov 27, 2020 08:31:07.441884995 CET	55435	53	192.168.2.3	8.8.8.8
Nov 27, 2020 08:31:07.478748083 CET	53	55435	8.8.8.8	192.168.2.3
Nov 27, 2020 08:31:38.730645895 CET	50713	53	192.168.2.3	8.8.8.8
Nov 27, 2020 08:31:38.757855892 CET	53	50713	8.8.8.8	192.168.2.3
Nov 27, 2020 08:31:40.019184113 CET	56132	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 08:31:40.054466009 CET	53	56132	8.8.8.8	192.168.2.3
Nov 27, 2020 08:31:50.802264929 CET	58987	53	192.168.2.3	8.8.8.8
Nov 27, 2020 08:31:50.865437984 CET	53	58987	8.8.8.8	192.168.2.3
Nov 27, 2020 08:31:50.888202906 CET	56579	53	192.168.2.3	8.8.8.8
Nov 27, 2020 08:31:50.977401972 CET	53	56579	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 08:31:50.802264929 CET	192.168.2.3	8.8.8.8	0x4af0	Standard query (0)	mail.talleresgenerauto.es	A (IP address)	IN (0x0001)
Nov 27, 2020 08:31:50.888202906 CET	192.168.2.3	8.8.8.8	0x6d21	Standard query (0)	mail.talleresgenerauto.es	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 08:31:50.865437984 CET	8.8.8.8	192.168.2.3	0x4af0	No error (0)	mail.talleresgenerauto.es	talleresgenerauto.es		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 08:31:50.865437984 CET	8.8.8.8	192.168.2.3	0x4af0	No error (0)	talleresgenerauto.es		217.61.130.138	A (IP address)	IN (0x0001)
Nov 27, 2020 08:31:50.977401972 CET	8.8.8.8	192.168.2.3	0x6d21	No error (0)	mail.talleresgenerauto.es	talleresgenerauto.es		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 08:31:50.977401972 CET	8.8.8.8	192.168.2.3	0x6d21	No error (0)	talleresgenerauto.es		217.61.130.138	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 27, 2020 08:31:51.319319963 CET	587	49740	217.61.130.138	192.168.2.3	220-pantallazoazul.zonasprivadasdns.com ESMTP Exim 4.93 #2 Fri, 27 Nov 2020 08:31:51 +0100 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 27, 2020 08:31:51.319869041 CET	49740	587	192.168.2.3	217.61.130.138	EHLO 745773
Nov 27, 2020 08:31:51.372632027 CET	587	49740	217.61.130.138	192.168.2.3	250-pantallazoazul.zonasprivadasdns.com Hello 745773 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 27, 2020 08:31:51.373213053 CET	49740	587	192.168.2.3	217.61.130.138	STARTTLS
Nov 27, 2020 08:31:51.430037022 CET	587	49740	217.61.130.138	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior

- AWB-18267638920511_ES.exe
- schtasks.exe
- conhost.exe
- AWB-18267638920511_ES.exe

Click to jump to process

System Behavior

Analysis Process: AWB-18267638920511_ES.exe PID: 3984 Parent PID: 5724

General

Start time:	08:30:04
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\AWB-18267638920511_ES.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\AWB-18267638920511_ES.exe'
Imagebase:	0xdc0000
File size:	531456 bytes
MD5 hash:	8B7F30A440FCC0B4B4EA690ECBFFF43E
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: 00000000.00000002.223775772.00000000042A4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.224015893.000000000449F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.223047556.0000000003201000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DE9CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DE9CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\tGjZeZC.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CCE1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpA7E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CCE7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AWB-18267638920511_ES.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1AC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA7E.tmp	success or wait	1	6CCE6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\tGjZeZC.exe	unknown	531456	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 67 07 be 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 12 08 00 00 08 00 00 00 00 00 00 3e 30 08 00 00 20 00 00 00 40 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...g.._.......... ....>0... ...@....@.. ....@.................	success or wait	1	6CCE1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA7E.tmp	unknown	1640	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6CCE1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AWB-18267638920511_ES.exe.log	unknown	1393	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, 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_v4.0.3	success or wait	1	6E1AC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE7CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCE1B4F	ReadFile
C:\Users\user\Desktop\AWB-18267638920511_ES.exe	unknown	531456	success or wait	1	6CCE1B4F	ReadFile

Analysis Process: schtasks.exe PID: 5944 Parent PID: 3984

General

Start time:	08:30:11
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\tGjZeZC' /XML 'C:\Users\ user\AppData\Local\Temp\tmpA7E.tmp'
Imagebase:	0x11c0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA7E.tmp	unknown	2	success or wait	1	11CAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA7E.tmp	unknown	1641	success or wait	1	11CABD9	ReadFile

Analysis Process: conhost.exe PID: 6140 Parent PID: 5944

General

Start time:	08:30:11
Start date:	27/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: AWB-18267638920511_ES.exe PID: 3728 Parent PID: 3984

General

Start time:	08:30:12
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\AWB-18267638920511_ES.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xa90000
File size:	531456 bytes
MD5 hash:	8B7F30A440FCC0B4B4EA690ECBFFF43E
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: 00000003.00000002.470115094.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.474541903.0000000002DF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.474541903.0000000002DF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.475012814.0000000002EA4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.475012814.0000000002EA4000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DE9CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DE9CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE75705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCE1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CCE1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CCE1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CCE1B4F	ReadFile

Disassembly

Code Analysis