ID: 379730
Sample Name: AMPUTERE.exe
Cookbook: default.jbs
Time: 07:40:53
Date: 01/04/2021
Version: 31.0.0 Emerald

Table of Contents

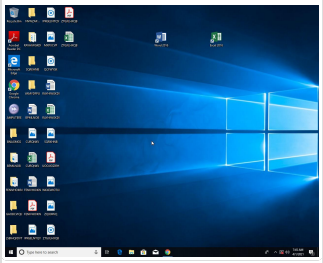
Analysis Report AMPUTERE.exe

Overview

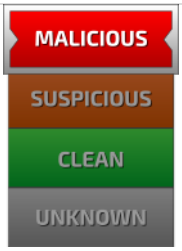
General Information

Sample Name:	AMPUTERE.exe
Analysis ID:	379730
MD5:	f2fa3c87de32858..
SHA1:	3d6f6d635639c68.
SHA256:	2beda3caff1f808…
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection



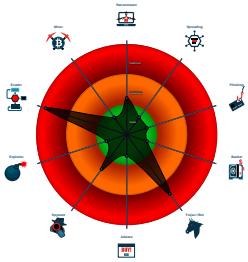
AgentTesla GuLoader

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

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected GuLoader
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Writes to foreign memory regions

Classification



Startup

- **System is w10x64**
- AMPUTERE.exe (PID: 6608 cmdline: 'C:\Users\user\Desktop\AMPUTERE.exe' MD5: F2FA3C87DE32858F1244FB352873F399)
  - RegAsm.exe (PID: 6044 cmdline: 'C:\Users\user\Desktop\AMPUTERE.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - conhost.exe (PID: 1212 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

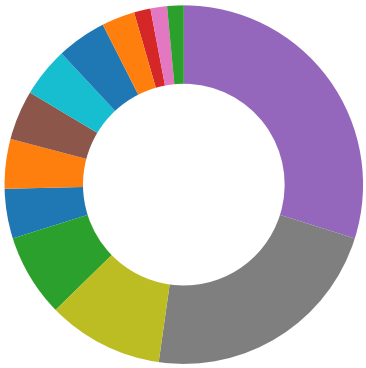
Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.864518316.000000001DEE1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000013.00000002.864518316.000000001DEE1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000013.00000002.859923887.000000000110 2000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: RegAsm.exe PID: 6044	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: RegAsm.exe PID: 6044	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- 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

Click to jump to signature section

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Multi AV Scanner detection for submitted file
- Machine Learning detection for sample

Data Obfuscation:

- Yara detected GuLoader

Malware Analysis System Evasion:

- Contains functionality to detect hardware virtualization (CPUID execution measurement)
- Detected RDTSC dummy instruction sequence (likely for instruction hammering)
- Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)
- Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)
- Tries to detect Any.run
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

- Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

- Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

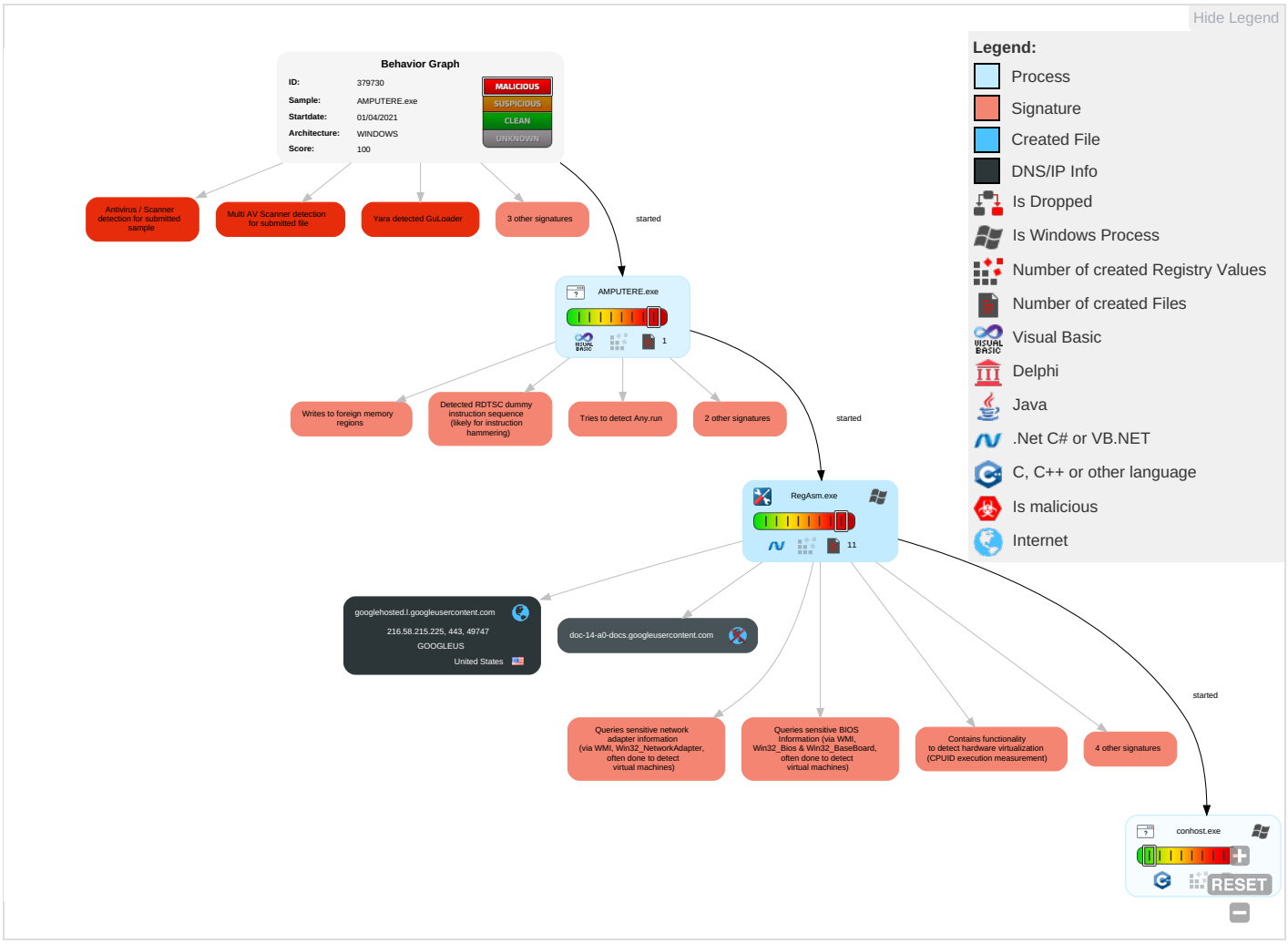
Remote Access Functionality:

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	DLL Side-Loading 1	Access Token Manipulation 1	Disable or Modify Tools 1	Input Capture 1	Security Software Discovery 7 3 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	E I N C
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Virtualization/Sandbox Evasion 3 4 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	E F C
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Access Token Manipulation 1	Security Account Manager	Virtualization/Sandbox Evasion 3 4 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	System Information Discovery 4 2 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S

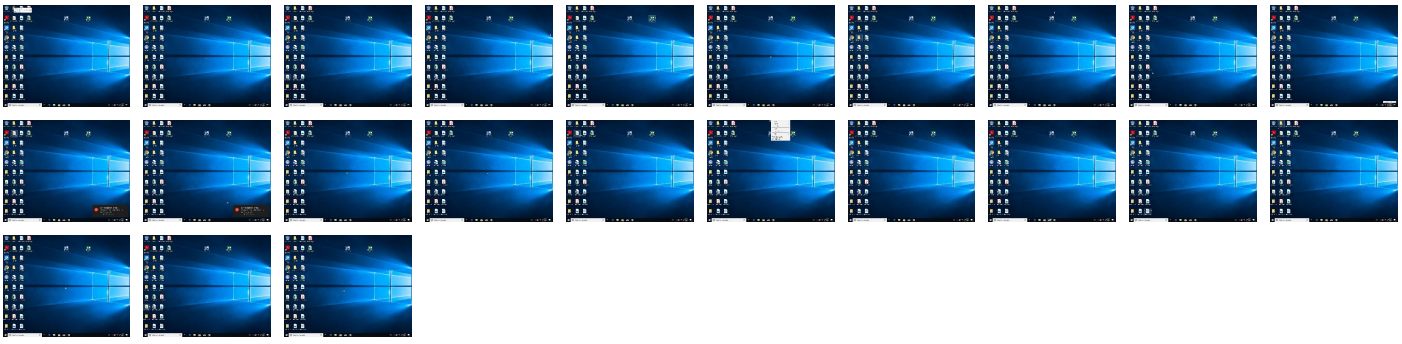
Behavior Graph



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
AMPUTERE.exe	45%	Virustotal		Browse
AMPUTERE.exe	69%	ReversingLabs	Win32.Trojan.GenericML	
AMPUTERE.exe	100%	Avira	HEUR/AGEN.1138570	
AMPUTERE.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.AMPUTERE.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138570		Download File
0.0.AMPUTERE.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138570		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://CFlLIU.com	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://DynDns.comDynDNS	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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	

Domains and IPs

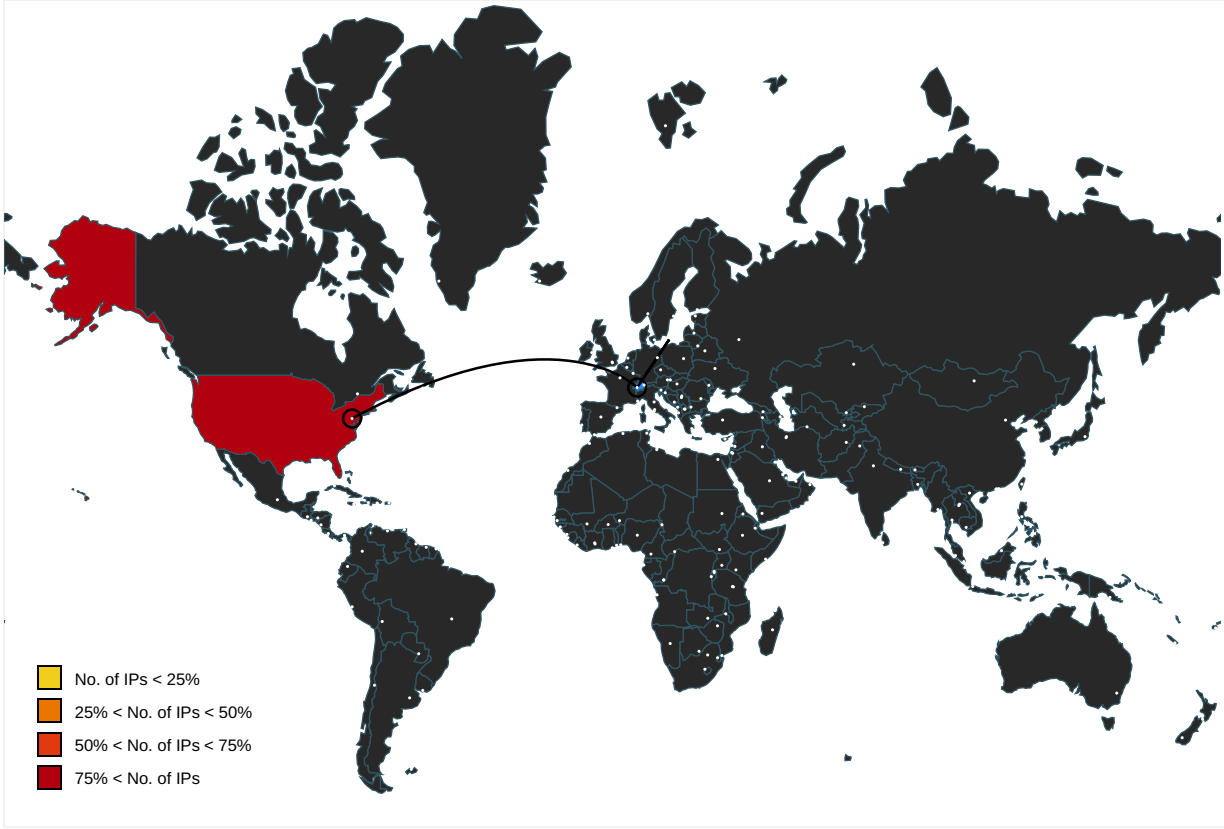
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
googlehosted.l.googleusercontent.com	216.58.215.225	true	false		high
doc-14-a0-docs.googleusercontent.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 00000013.00000002.864518316.000000001DEE1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://CFlLIU.com	RegAsm.exe, 00000013.00000002.864518316.000000001DEE1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNS	RegAsm.exe, 00000013.00000002.864518316.000000001DEE1000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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	RegAsm.exe, 00000013.00000002.864518316.000000001DEE1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.215.225	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	379730
Start date:	01.04.2021
Start time:	07:40:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AMPUTERE.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@4/0@1/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 95.9% (good quality ratio 37%) • Quality average: 21.8% • Quality standard deviation: 30.5%
HCA Information:	• Successful, ratio: 87% • 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 • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.43.193.48, 168.61.161.212, 13.107.4.50, 104.43.139.144, 40.88.32.150, 20.82.210.154, 2.20.142.210, 2.20.142.209, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247, 23.218.208.56, 216.58.215.238 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, 2-01-3cf7-0009.cdx.cedexis.net, b1ns.c-0001.c-msedge.net, wu-fg-shim.trafficmanager.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, drive.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, b1ns.au-msedge.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, c-0001.c-msedge.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, download.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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.

Simulations

Behavior and APIs

Time	Type	Description
07:45:34	API Interceptor	158x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	martin.connor SWIFT Copy 2021.htm	Get hash	malicious	Browse	• 216.58.215.225
	xXeJaeHDWB.exe	Get hash	malicious	Browse	• 216.58.215.225
	Purchase_Order 3109.xls	Get hash	malicious	Browse	• 216.58.215.225
	Invoice_150.xlsm	Get hash	malicious	Browse	• 216.58.215.225
	FileZilla_3.53.1_win64_sponsored-setup.exe	Get hash	malicious	Browse	• 216.58.215.225
	#Ufffd.HTML	Get hash	malicious	Browse	• 216.58.215.225
	FileZilla_3.53.1_win64_sponsored-setup.exe	Get hash	malicious	Browse	• 216.58.215.225
	SecuriteInfo.com.Mal.GandCrypt-A.4160.exe	Get hash	malicious	Browse	• 216.58.215.225
	1Nqs1iTfMz.exe	Get hash	malicious	Browse	• 216.58.215.225
	yPkfbflyoh.exe	Get hash	malicious	Browse	• 216.58.215.225
	SOC_0#7198, INV#512 Via GoogleDocs gracechung.html	Get hash	malicious	Browse	• 216.58.215.225
	lv.exe	Get hash	malicious	Browse	• 216.58.215.225
	8637.xlsx	Get hash	malicious	Browse	• 216.58.215.225
	YtR0OI1H6G.exe	Get hash	malicious	Browse	• 216.58.215.225
	ABS Browser.exe	Get hash	malicious	Browse	• 216.58.215.225
	reciept-id.htm	Get hash	malicious	Browse	• 216.58.215.225
	Closure TP-Stamp.htm	Get hash	malicious	Browse	• 216.58.215.225
	Audio playback (7656) for joew Camrosa.htm	Get hash	malicious	Browse	• 216.58.215.225
	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe	Get hash	malicious	Browse	• 216.58.215.225
	JYDy1dAHdW.exe	Get hash	malicious	Browse	• 216.58.215.225

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.402488868367982
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	AMPUTERE.exe
File size:	90112

General

MD5:	f2fa3c87de32858f1244fb352873f399
SHA1:	3d6f6d635639c689a8e4709ccb379500b4e76096
SHA256:	2beda3caff1f808814294dca346cbe62ad229272d54696fe75e99388a73ff3cc
SHA512:	46058516a19a7db0833fd84a17ab9f8a80b992e6ac7672 abe879dd1bf2e5a04636b7436746b5a472dd67c1efa42a 07a88779a2f1f6ec12d431a6be8a13a605
SSDEEP:	768:xKOhTQs/sICfEBiQPIHYqH3qkfNS1Z5EK8GEHPZNrLzrKBvY:1hkGxCfEBiiljHBG8tHC
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~...0.....0...Rich1.....PE..L.....T.....0.....0....@.....

File Icon

Icon Hash:	f1f8f6f0f0e4f831

Static PE Info

General

Entrypoint:	0x4016fc
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:	
Time Stamp:	0x540DA20E [Mon Sep 8 12:33:18 2014 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:	c78f78af0a4b82efe93f926bf0040578

Entrypoint Preview

Instruction
push 0040CE4Ch
call 00007F9984FBFCD5h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
dec eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dl, al
push eax

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x11ec4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x14000	0x1412	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1ac	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x114d8	0x12000	False	0.434828016493	data	5.9787925967	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x13000	0xa64	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x14000	0x1412	0x2000	False	0.291259765625	data	3.29525991326	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x14d4a	0x6c8	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x143c2	0x988	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0x143a0	0x22	data		
RT_VERSION	0x14120	0x280	data	Guarani	Paraguay

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaAryMove, __vbaLenBstr, __vbaStrVarMove, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaSetSystemError, __vbaHresultCheckObj, __vbaLenBstrB, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR8, __vbaVarTstLt, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaObjVar, DllFunctionCall, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaDateVar, _CIlog, __vbaFileOpen, __vbaNew2, __vbaInStr, __vbaVar2Vec, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaLateMemCall, __vbaVarAdd, __vbaStrToAnsi, __vbaVarDup, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaStrMove, __vbaUI1Str, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0474 0x04b0
InternalName	AMPUTERE
FileVersion	3.03
CompanyName	Panasonic
Comments	Panasonic
ProductName	Panasonic
ProductVersion	3.03
FileDescription	Panasonic
OriginalFilename	AMPUTERE.exe

Possible Origin

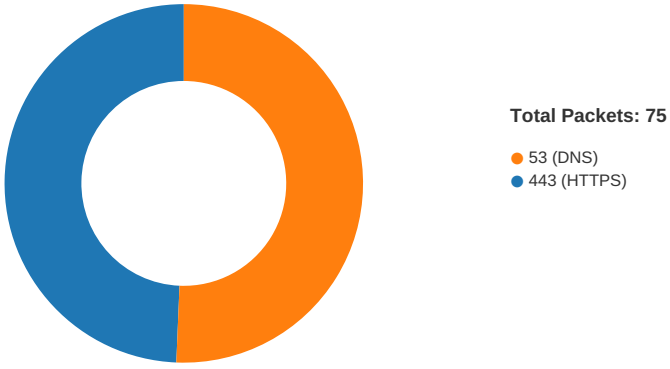
Language of compilation system	Country where language is spoken	Map
Guarani	Paraguay	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/01/21-07:41:42.432040	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/01/21-07:41:42.464302	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
04/01/21-07:41:42.470500	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/01/21-07:41:42.502832	ICMP	449	ICMP Time-To-Live Exceeded in Transit			5.56.20.161	192.168.2.6
04/01/21-07:41:42.506701	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/01/21-07:41:42.540227	ICMP	449	ICMP Time-To-Live Exceeded in Transit			91.206.52.152	192.168.2.6
04/01/21-07:41:42.540792	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/01/21-07:41:46.555734	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/01/21-07:41:50.533063	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/01/21-07:41:54.533682	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/01/21-07:41:58.533986	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/01/21-07:42:03.273472	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/01/21-07:42:07.040459	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/01/21-07:42:11.039405	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/01/21-07:42:15.035238	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/01/21-07:42:19.071881	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/01/21-07:42:23.036318	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/01/21-07:42:27.037681	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/01/21-07:42:31.036811	ICMP	384	ICMP PING			192.168.2.6	13.107.4.50
04/01/21-07:42:31.069811	ICMP	408	ICMP Echo Reply			13.107.4.50	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 1, 2021 07:45:26.435566902 CEST	49747	443	192.168.2.6	216.58.215.225

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 1, 2021 07:45:26.478147984 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.478259087 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.479070902 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.521552086 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.534030914 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.534054041 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.534066916 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.534079075 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.534224033 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.551301003 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.594008923 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.594080925 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.594995022 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.642653942 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.876184940 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.876216888 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.876230955 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.876246929 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.876261950 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.876364946 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.876398087 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.879012108 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.879033089 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.879138947 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.882077932 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.882103920 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.882241964 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.885045052 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.885070086 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.885191917 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.888066053 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.888092041 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.888215065 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.896469116 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.896631002 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.897058010 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.897149086 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.920533895 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.920563936 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.920715094 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.921978951 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.922003031 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.922103882 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.924967051 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.924994946 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.925097942 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.927953005 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.927983999 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.928090096 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.930926085 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.930965900 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.931082964 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.933958054 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.933989048 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.934043884 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.934098959 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.936952114 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.937001944 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.937047005 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.937093973 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.939922094 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.939948082 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.940052032 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.942869902 CEST	443	49747	216.58.215.225	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 1, 2021 07:45:26.942890882 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.943018913 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.945904970 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.945930004 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.946086884 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.948846102 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.948868036 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.948987007 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.951828003 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.951868057 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.951960087 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.954854012 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.954925060 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.954963923 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.954986095 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.957878113 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.957906961 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.957998037 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.960839033 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.960863113 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.960953951 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.964852095 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.964884996 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.965053082 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.966298103 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.966320992 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.966459990 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.968224049 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.968250036 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.968362093 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.970232964 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.970264912 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.970804930 CEST	49747	443	192.168.2.6	216.58.215.225
Apr 1, 2021 07:45:26.972218037 CEST	443	49747	216.58.215.225	192.168.2.6
Apr 1, 2021 07:45:26.972256899 CEST	443	49747	216.58.215.225	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 1, 2021 07:41:38.070863008 CEST	54513	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:41:38.118454933 CEST	53	54513	8.8.8.8	192.168.2.6
Apr 1, 2021 07:41:38.879174948 CEST	62044	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:41:38.929502964 CEST	53	62044	8.8.8.8	192.168.2.6
Apr 1, 2021 07:41:39.825949907 CEST	63791	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:41:39.876066923 CEST	53	63791	8.8.8.8	192.168.2.6
Apr 1, 2021 07:41:41.726422071 CEST	64267	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:41:41.783688068 CEST	53	64267	8.8.8.8	192.168.2.6
Apr 1, 2021 07:41:42.364645004 CEST	49448	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:41:42.421184063 CEST	53	49448	8.8.8.8	192.168.2.6
Apr 1, 2021 07:41:43.635649920 CEST	60342	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:41:43.685589075 CEST	53	60342	8.8.8.8	192.168.2.6
Apr 1, 2021 07:41:51.600878000 CEST	61346	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:41:51.649561882 CEST	53	61346	8.8.8.8	192.168.2.6
Apr 1, 2021 07:41:52.768568993 CEST	51774	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:41:52.816342115 CEST	53	51774	8.8.8.8	192.168.2.6
Apr 1, 2021 07:41:53.692286968 CEST	56023	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:41:53.739046097 CEST	53	56023	8.8.8.8	192.168.2.6
Apr 1, 2021 07:41:54.686860085 CEST	58384	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:41:54.735239983 CEST	53	58384	8.8.8.8	192.168.2.6
Apr 1, 2021 07:41:56.208642006 CEST	60261	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:41:56.254461050 CEST	53	60261	8.8.8.8	192.168.2.6
Apr 1, 2021 07:41:57.274804115 CEST	56061	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:41:57.323487997 CEST	53	56061	8.8.8.8	192.168.2.6
Apr 1, 2021 07:41:58.575582027 CEST	58336	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 1, 2021 07:41:58.622155905 CEST	53	58336	8.8.8.8	192.168.2.6
Apr 1, 2021 07:41:59.844504118 CEST	53781	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:41:59.893209934 CEST	53	53781	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:04.149950981 CEST	54064	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:04.195872068 CEST	53	54064	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:05.189529896 CEST	52811	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:05.237653017 CEST	53	52811	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:07.419472933 CEST	55299	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:07.465405941 CEST	53	55299	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:08.486334085 CEST	63745	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:08.532182932 CEST	53	63745	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:09.296761036 CEST	50055	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:09.344470978 CEST	53	50055	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:11.085506916 CEST	61374	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:11.141558886 CEST	53	61374	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:33.522531986 CEST	50339	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:33.589736938 CEST	53	50339	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:35.327601910 CEST	63307	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:35.482263088 CEST	53	63307	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:36.180342913 CEST	49694	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:36.237016916 CEST	53	49694	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:37.043318987 CEST	54982	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:37.097539902 CEST	53	54982	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:37.534673929 CEST	50010	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:37.628061056 CEST	53	50010	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:38.209295988 CEST	63718	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:38.255273104 CEST	53	63718	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:38.802638054 CEST	62116	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:38.859879017 CEST	53	62116	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:39.162408113 CEST	63816	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:39.230982065 CEST	53	63816	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:39.300668955 CEST	55014	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:39.355036974 CEST	53	55014	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:40.345225096 CEST	62208	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:40.391186953 CEST	53	62208	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:41.812714100 CEST	57574	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:41.859698057 CEST	53	57574	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:42.381419897 CEST	51818	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:42.437664986 CEST	53	51818	8.8.8.8	192.168.2.6
Apr 1, 2021 07:42:56.505729914 CEST	56628	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:42:56.561142921 CEST	53	56628	8.8.8.8	192.168.2.6
Apr 1, 2021 07:43:14.194900990 CEST	60778	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:43:14.252999067 CEST	53	60778	8.8.8.8	192.168.2.6
Apr 1, 2021 07:43:22.684170961 CEST	53799	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:43:22.733340979 CEST	53	53799	8.8.8.8	192.168.2.6
Apr 1, 2021 07:43:28.743518114 CEST	54683	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:43:28.814992905 CEST	53	54683	8.8.8.8	192.168.2.6
Apr 1, 2021 07:45:25.612718105 CEST	59329	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:45:25.678809881 CEST	53	59329	8.8.8.8	192.168.2.6
Apr 1, 2021 07:45:26.367213011 CEST	64021	53	192.168.2.6	8.8.8.8
Apr 1, 2021 07:45:26.431298018 CEST	53	64021	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 1, 2021 07:45:26.367213011 CEST	192.168.2.6	8.8.8.8	0xfc91	Standard query (0)	doc-14-a0-docs.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 1, 2021 07:45:26.431298018 CEST	8.8.8.8	192.168.2.6	0xfc91	No error (0)	doc-14-a0-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 1, 2021 07:45:26.431298018 CEST	8.8.8.8	192.168.2.6	0xfc91	No error (0)	googlehosted.l.googleusercontent.com		216.58.215.225	A (IP address)	IN (0x0001)

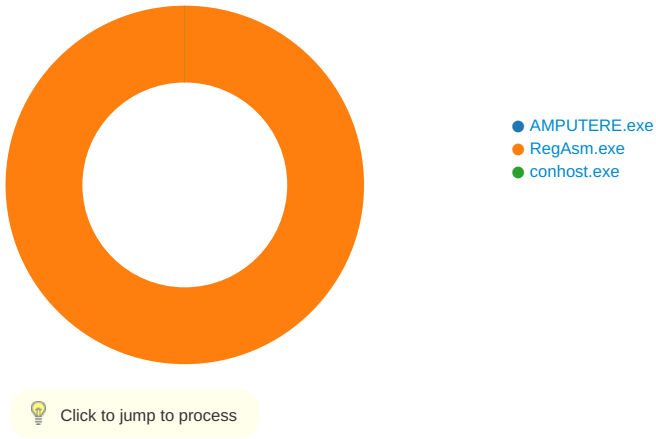
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 1, 2021 07:45:26.534079075 CEST	216.58.215.225	443	192.168.2.6	49747	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Mar 16 20:32:57 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jun 08 21:32:56 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: AMPUTERE.exe PID: 6608 Parent PID: 5964

General

Start time:	07:41:46
Start date:	01/04/2021
Path:	C:\Users\user\Desktop\AMPUTERE.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\AMPUTERE.exe'

Imagebase:	0x400000
File size:	90112 bytes
MD5 hash:	F2FA3C87DE32858F1244FB352873F399
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 6044 Parent PID: 6608

General

Start time:	07:45:13
Start date:	01/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\AMPUTERE.exe'
Imagebase:	0xd30000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
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: 00000013.00000002.864518316.000000001DEE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000013.00000002.864518316.000000001DEE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000013.00000002.859923887.0000000001102000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

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	1103D8B	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1103D8B	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1103D8B	InternetOpenUrlA

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	1103D8B	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1103D8B	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1103D8B	InternetOpenUrlA
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	72FB60AC	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	72FB60AC	unknown
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	72FB60AC	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	72FB60AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown

Analysis Process: conhost.exe PID: 1212 Parent PID: 6044

General

Start time:	07:45:13
Start date:	01/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff614b90000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis