ID: 532886
Sample Name: Image001.exe
Cookbook: default.jbs
Time: 19:23:33
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

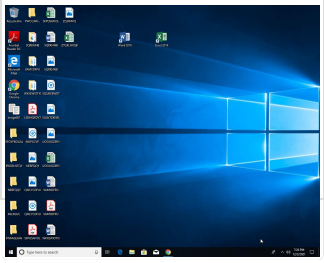
Windows Analysis Report Image001.exe

Overview

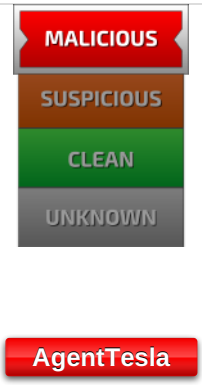
General Information

Sample Name:	Image001.exe
Analysis ID:	532886
MD5:	ff1b46d412d2890..
SHA1:	2c2c60bc32b11f8..
SHA256:	3f9f72ec6bd7595..
Tags:	agenttesla exe
Infos:	

Most interesting Screenshot:



Detection



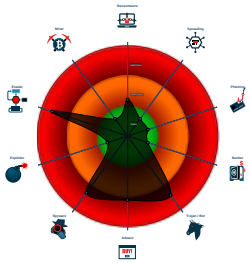
AgentTesla

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Detected unpacking (creates a PE fi…
- Tries to steal Mail credentials (via fil…
- Initial sample is a PE file and has a …
- Tries to harvest and steal ftp login c…
- Modifies the hosts file
- Injects a PE file into a foreign proce…
- .NET source code contains very larg…
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- Image001.exe (PID: 3524 cmdline: "C:\Users\user\Desktop\Image001.exe" MD5: FF1B46D412D2890828FDEEE1D983DEA1)
  - Image001.exe (PID: 6004 cmdline: "C:\Users\user\Desktop\Image001.exe" MD5: FF1B46D412D2890828FDEEE1D983DEA1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "castilloo@cgyasc.com",
  "Password": "Castle1",
  "Host": "mail.cgyasc.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.929244292.000000000400000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.929244292.000000000400000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000002.931306389.00000000047B0000.00000004.00020000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.931306389.00000000047B0000.00000004.00020000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000002.929487870.0000000000620000.00000004.00000020.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 19 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.Image001.exe.647018.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.Image001.exe.647018.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.2.Image001.exe.47b0000.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.Image001.exe.47b0000.4.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.2.Image001.exe.47b0000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 55 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Compliance:

Detected unpacking (creates a PE file in dynamic memory)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Data Obfuscation:

Detected unpacking (creates a PE file in dynamic memory)

Malware Analysis System Evasion:

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

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

HIPS / PFW / Operating System Protection Evasion:

- Modifies the hosts file
- Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings:

- Modifies the hosts file

Stealing of Sensitive Information:

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

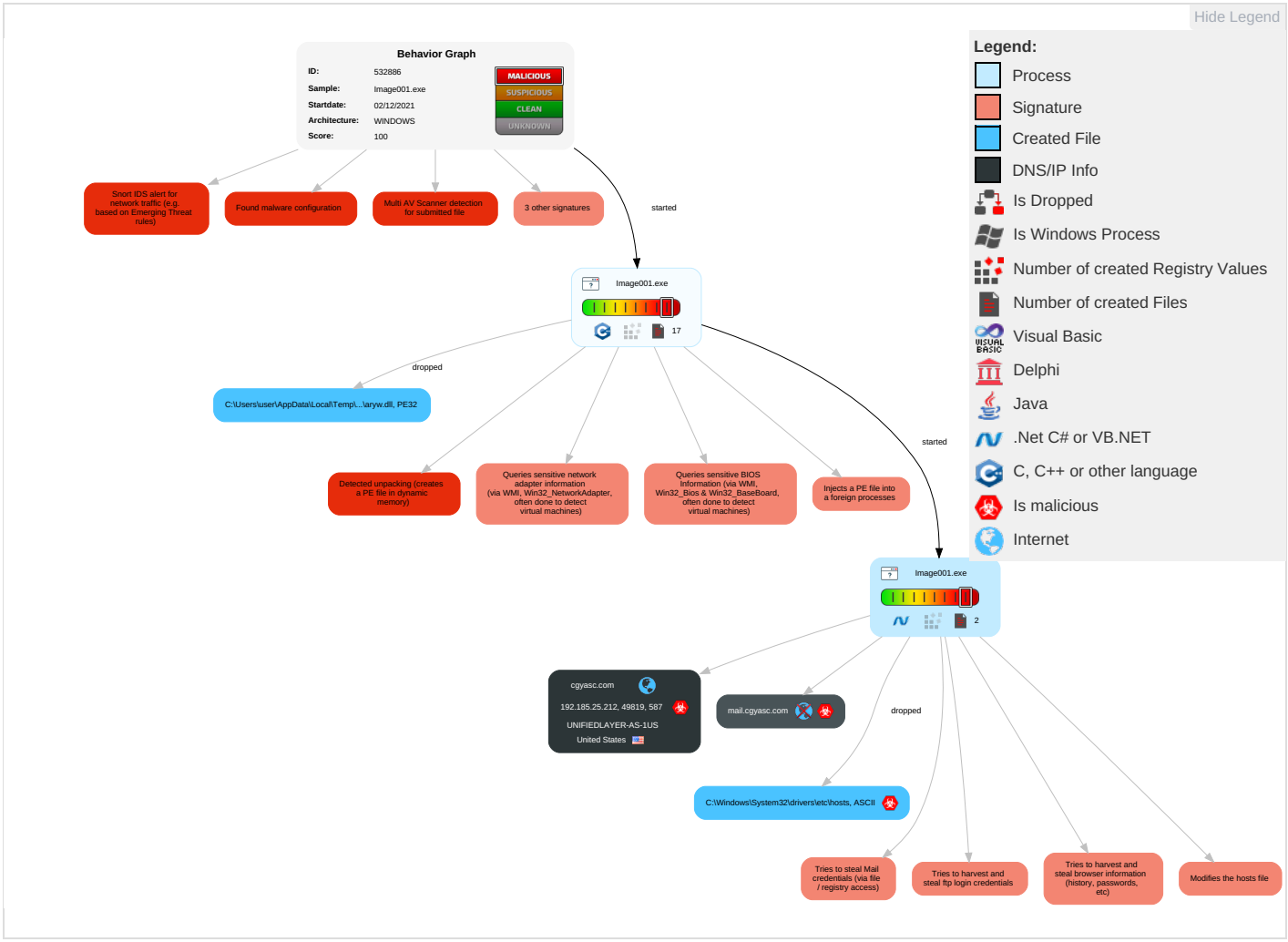
Remote Access Functionality:

- 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 2 1 1	Path Interception	Process Injection 1 1 2	File and Directory Permissions Modification 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	System Information Discovery 1 2 7	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Query Registry 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Protocol Impersonatio
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 1	LSA Secrets	Security Software Discovery 1 4 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Virtualization/Sandbox Evasion 1 3 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	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocol

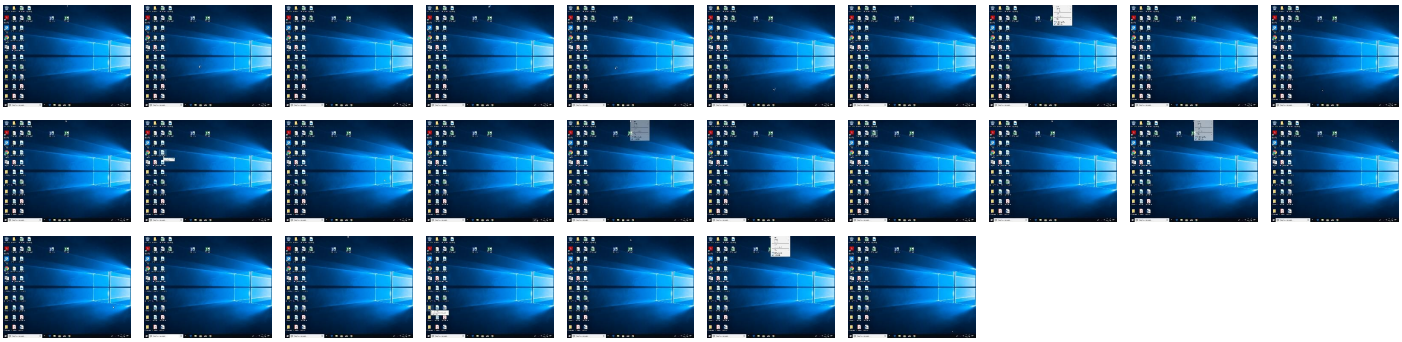
Behavior Graph



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
Image001.exe	33%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsnD9EC.tmp\aryw.dll	7%	ReversingLabs	Win32.Trojan.InjectorAGen	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.1.Image001.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.Image001.exe.400000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.2.Image001.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.Image001.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.Image001.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.Image001.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.Image001.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.2.Image001.exe.4810000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.Image001.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.Image001.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
cgyasc.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://mail.cgyasc.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://YcxkAh.com	0%	Avira URL Cloud	safe	
http://cgyasc.com	0%	Avira URL Cloud	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	0%	URL Reputation	safe	
http://9zUeuRC8ZtAGmU0.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cgyasc.com	192.185.25.212	true	true	• 0%, Virustotal, Browse	unknown
mail.cgyasc.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.25.212	cgyasc.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532886
Start date:	02.12.2021
Start time:	19:23:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Image001.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:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.evad.winEXE@3/3@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.1% (good quality ratio 7.5%) • Quality average: 77.6% • Quality standard deviation: 30.5%
HCA Information:	• Successful, ratio: 89% • 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

Simulations

Behavior and APIs

Time	Type	Description
19:24:43	API Interceptor	701x Sleep call for process: Image001.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	Solicitud urgente de Quotaion_U1197,pdf.exe	Get hash	malicious	Browse	• 162.214.233.244
	OSCBLUS33XXX1032021110200150939.exe	Get hash	malicious	Browse	• 192.185.224.36
	RFQ - SST#2021111503.exe	Get hash	malicious	Browse	• 162.241.253.162
	ufKi6DmWMQCuEb4.exe	Get hash	malicious	Browse	• 192.185.16.241
	counter-1248368226.xls	Get hash	malicious	Browse	• 108.179.192.98
	counter-1248368226.xls	Get hash	malicious	Browse	• 108.179.192.98
	counter-1248368226.xls	Get hash	malicious	Browse	• 108.179.192.98
	counter-1248368226.xls	Get hash	malicious	Browse	• 108.179.192.98
	CU-6431 report.xlsm	Get hash	malicious	Browse	• 162.240.9.126
	CU-6431 report.xlsm	Get hash	malicious	Browse	• 162.240.9.126
	DkX9HVJTmi.exe	Get hash	malicious	Browse	• 108.167.135.122
	Shipping report -17420.xlsx	Get hash	malicious	Browse	• 162.241.169.32
	SCAN_7295943480515097.xlsm	Get hash	malicious	Browse	• 162.240.9.126
	SCAN_7295943480515097.xlsm	Get hash	malicious	Browse	• 162.240.9.126
	INVOICE.exe	Get hash	malicious	Browse	• 162.214.80.6
	img20048901738_Pago.pdf.exe	Get hash	malicious	Browse	• 192.185.115.3
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	• 162.241.126.156
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	• 162.241.126.156
	New order documents. pdf.....exe	Get hash	malicious	Browse	• 108.179.232.76
	part-1500645108.xlsb	Get hash	malicious	Browse	• 162.241.62.201

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\a6anvv1jtgu	
Process:	C:\Users\user\Desktop\Image001.exe
File Type:	data
Category:	dropped
Size (bytes):	292863
Entropy (8bit):	7.9590314200515655
Encrypted:	false
SSDEEP:	6144:GenN8Knw1VmqeiSNa7vDCPt1Vd3R12NAuo:Gaw1VmqeJNEbCPt1HR6e
MD5:	E33BFE017932FC9BD96B243B5A64D532
SHA1:	270699A71319AF947553F53BAA5507963DFAC800
SHA-256:	B77A107EBC3C235287A4625A4ABC454AD6159B46532B1DC6EE6F8A0B49B5DDB4
SHA-512:	1E5774D7D932445A8FED129926EE203937310592423EF7D378819CAE98DEA4505A829BB3F8F0CB9BB3D2A9CAAD48F02C6A1D2F91CD30E2EEB2BD79B471CE961
Malicious:	false
Reputation:	low
Preview:	#...).\....?.y..t2.....h.c.]...@.b..g...@..q.(..E.S...y.uO`.V..Bi...QX.{-.z.0.g8u.d.....W.P.....t...;>;.....B..6.....e..1.Cp.c.8.m..z.x.o..=c...._S..U.w..#...3._....^.G.b.'.....D..F..W.>...`s....-.au[...JlhH..h.j.H..7...T..;y..d...\....?.8e..Z2D.....[...@.b...o..@....(....S.-..Z..O.....WW.Q..1....H..+..Lo.....Q0..,4...+....k.S.](.T.r..Bv.6.V..zf-%.$....e....M.....z ...V.....-....2....?.)..T..<...A.$P..{....B..P3.....H_..l.V.]..O.....&..(.....r..T..;y...Q.\..v.?.Z.....h.c.].....bP.!.g.....(..F.S....ZluO.u...+.W..M..1..e....+...Z....S...0....+....k.S..(o...VW.8Y.6._..zf...Mkp...y..tM..&.... ..].NL.eV.....-.vr.....M..)..T..<...A.#P..{....B..3.....H_..l.V.].....&..(.....r..T..;y..d...\....?...2.....h.c.]...@.b..g...@..q.(..E.S...Z.uO.u...+.W..M..1....+..L...d...Q0..4...+....k.S..(...r..B..6.V..zf-%.M.p..e..tM..&.....z ...V.....-.....?.)..T..<...A.$P..{....B..3.....H_..l.V.].....

C:\Users\user\AppData\Local\Temp\nsnD9EC.tmp\aryw.dll	
Process:	C:\Users\user\Desktop\Image001.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	166400
Entropy (8bit):	6.376105999975598
Encrypted:	false
SSDEEP:	3072:8ScpBPEbLSQsIIipXcvowrbXbQJUB0ElFyot9:8SoB8oIxALQmz
MD5:	B1D39A59ACC5C67685D5898E25AD7874
SHA1:	C71B2D3960DAEC838CA13CD4890B1F4D1589B09B
SHA-256:	0A94E73C19307113508E6A6103EF6ABFE7C77BC61BE29ECA172C97F86FDDB6CC
SHA-512:	E71C6DDD29A41F358C5667F667606A9EF1AA1334AC6CE3059B7B81F34279482BCF24E90C74416FBE088103D1D2C4AC048E8A74B82BFF414DCE86AF2EA67F045
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 7%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A..$...w...w...w...w$..w..*w...w...wj..w...v...w...v...w...w...w...v...w...v...w...v...wRich...w.....PE..L...A..a.....!..... .....e.....\f.....``.....`..@..... ..l.....text...L..... ..`.rdata...S... ...T.....@..@.data....B.....&...b.....@....rsrc.....@..@.....

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Users\user\Desktop\Image001.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB

C:\Windows\System32\drivers\etc\hosts	
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA2
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.229239721188142
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	Image001.exe
File size:	627403
MD5:	ff1b46d412d2890828fdeee1d983dea1
SHA1:	2c2c60bc32b11f866aed66f29ce30c362b352567
SHA256:	3f9f72ec6bd759569e783528a4a2e0426472dfae328af93afbf9da273e92adf5
SHA512:	d6ea42338428fc9da1552c1879b334b4a70f121eb9c3fce31b513bc86f2eca5a7ba7bb17a6ec059910b2fda3f2bb6717a975828f6de985630d0420bde153333b
SSDEEP:	12288:ZNdrZZ0XO9DUtlQJt58bW7V75KoxcVag+Mf3/+:ndrXI0gXQJt5WWR75Zxst+
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....\.....0.....

File Icon

Icon Hash:	32b28a9a9a9a9290

Static PE Info

General

Entrypoint:	0x4030e3
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:	0x48EFCDCD [Fri Oct 10 21:49:01 2008 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

General

Import Hash:	7fa974366048f9c551ef45714595665e

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5b68	0x5c00	False	0.67722486413	data	6.48746502716	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x129c	0x1400	False	0.4337890625	data	5.04904254867	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x25c58	0x400	False	0.58203125	data	4.76995537906	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2f000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x37000	0x3c6c8	0x3c800	False	0.374326091167	data	5.60520303725	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-19:26:31.364161	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49819	587	192.168.2.4	192.185.25.212

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 19:26:29.583175898 CET	192.168.2.4	8.8.8.8	0xc0fd	Standard query (0)	mail.cgyasc.com	A (IP address)	IN (0x0001)
Dec 2, 2021 19:26:29.635986090 CET	192.168.2.4	8.8.8.8	0xb2f3	Standard query (0)	mail.cgyasc.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 19:26:29.601175070 CET	8.8.8.8	192.168.2.4	0xc0fd	No error (0)	mail.cgyasc.com	cgyasc.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 19:26:29.601175070 CET	8.8.8.8	192.168.2.4	0xc0fd	No error (0)	cgyasc.com		192.185.25.212	A (IP address)	IN (0x0001)
Dec 2, 2021 19:26:29.778151035 CET	8.8.8.8	192.168.2.4	0xb2f3	No error (0)	mail.cgyasc.com	cgyasc.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 19:26:29.778151035 CET	8.8.8.8	192.168.2.4	0xb2f3	No error (0)	cgyasc.com		192.185.25.212	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 2, 2021 19:26:30.303822994 CET	587	49819	192.185.25.212	192.168.2.4	220-elise.websitewelcome.com ESMTP Exim 4.94.2 #2 Thu, 02 Dec 2021 12:26:30 -0600 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Dec 2, 2021 19:26:30.304512024 CET	49819	587	192.168.2.4	192.185.25.212	EHLO 928100
Dec 2, 2021 19:26:30.458679914 CET	587	49819	192.185.25.212	192.168.2.4	250-elise.websitewelcome.com Hello 928100 [84.17.52.65] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Dec 2, 2021 19:26:30.459480047 CET	49819	587	192.168.2.4	192.185.25.212	AUTH login Y2FzdGlsbG9vQGNneWFzYy5jb20=
Dec 2, 2021 19:26:30.617846966 CET	587	49819	192.185.25.212	192.168.2.4	334 UGFzc3dvcmQ6
Dec 2, 2021 19:26:30.776721954 CET	587	49819	192.185.25.212	192.168.2.4	235 Authentication succeeded
Dec 2, 2021 19:26:30.778173923 CET	49819	587	192.168.2.4	192.185.25.212	MAIL FROM:<castilloo@cgyasc.com>
Dec 2, 2021 19:26:30.941581964 CET	587	49819	192.185.25.212	192.168.2.4	250 OK
Dec 2, 2021 19:26:30.941968918 CET	49819	587	192.168.2.4	192.185.25.212	RCPT TO:<mamaputmamaput175@gmail.com>
Dec 2, 2021 19:26:31.202622890 CET	587	49819	192.185.25.212	192.168.2.4	250 Accepted
Dec 2, 2021 19:26:31.202934980 CET	49819	587	192.168.2.4	192.185.25.212	DATA
Dec 2, 2021 19:26:31.362632036 CET	587	49819	192.185.25.212	192.168.2.4	354 Enter message, ending with "." on a line by itself
Dec 2, 2021 19:26:31.365576029 CET	49819	587	192.168.2.4	192.185.25.212	.
Dec 2, 2021 19:26:31.506036997 CET	587	49819	192.185.25.212	192.168.2.4	250 OK id=1msqmt-003gjG-94

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Image001.exe PID: 3524 Parent PID: 4488

General

Start time:	19:24:27
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\Image001.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Image001.exe"
Imagebase:	0x400000
File size:	627403 bytes
MD5 hash:	FF1B46D412D2890828FDEEE1D983DEA1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.674414732.0000000002960000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.674414732.0000000002960000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: Image001.exe PID: 6004 Parent PID: 3524

General

Start time:	19:24:29
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\Image001.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Image001.exe"
Imagebase:	0x400000
File size:	627403 bytes
MD5 hash:	FF1B46D412D2890828FDEEE1D983DEA1
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: 00000002.00000002.929244292.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.929244292.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.931306389.00000000047B0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.931306389.00000000047B0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.929487870.000000000062E000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.929487870.000000000062E000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.671627196.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.671627196.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.930135500.00000000022D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.930135500.00000000022D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.670129518.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.670129518.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.931937369.0000000004812000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.931937369.0000000004812000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.930749556.00000000032D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.930749556.00000000032D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000001.673527411.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000001.673527411.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.930497468.000000000260A000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis