ID: 553045
Sample Name: 8nZMrUpLlM
Cookbook: default.jbs
Time: 07:41:33
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

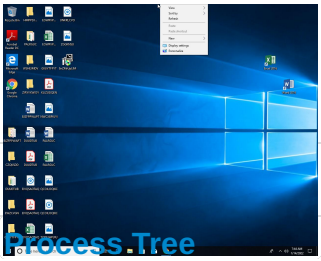
Table of Contents

Windows Analysis Report 8nZMrUpLlM

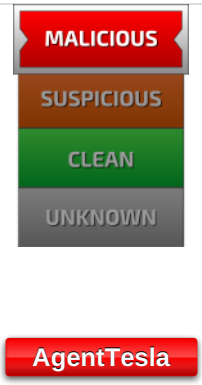
Overview

General Information

Sample Name:	8nZMrUpLlM (renamed file extension from none to exe)
Analysis ID:	553045
MD5:	8d58419427c916..
SHA1:	e787266ae57b7e..
SHA256:	9661e4c97ebfc0a..
Tags:	32 AgentTesla exe trojan
Infos:	
Most interesting Screenshot:	



Detection

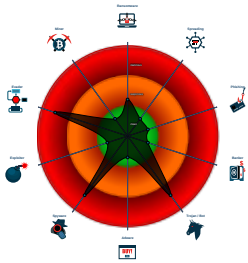


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Detected unpacking (creates a PE fi…
- Tries to steal Mail credentials (via fil…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Machine Learning detection for samp…
- Injects a PE file into a foreign proce…
- .NET source code contains very larg…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…

Classification



- **System is w10x64**
- 8nZMrUpLlM.exe (PID: 1056 cmdline: "C:\Users\user\Desktop\8nZMrUpLlM.exe" MD5: 8D58419427C9169B0894CEEE4659E905)
  - 8nZMrUpLlM.exe (PID: 4380 cmdline: "C:\Users\user\Desktop\8nZMrUpLlM.exe" MD5: 8D58419427C9169B0894CEEE4659E905)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "sales2@fttmas.com",
  "Password": "0*$]EwyY]^(?",
  "Host": "mail.fttmas.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.248124779.000000000304 0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.248124779.000000000304 0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000002.502323275.000000000040 0000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.502323275.000000000040 0000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000002.507139784.000000000498 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.8nZMrUpLIM.exe.3051458.5.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.8nZMrUpLIM.exe.3051458.5.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.8nZMrUpLIM.exe.3040000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.8nZMrUpLIM.exe.3040000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.0.8nZMrUpLIM.exe.415058.9.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 53 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

Machine Learning detection for sample

Compliance:

Detected unpacking (creates a PE file in dynamic memory)

System Summary:

.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:

Injects a PE file into a foreign processes

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)

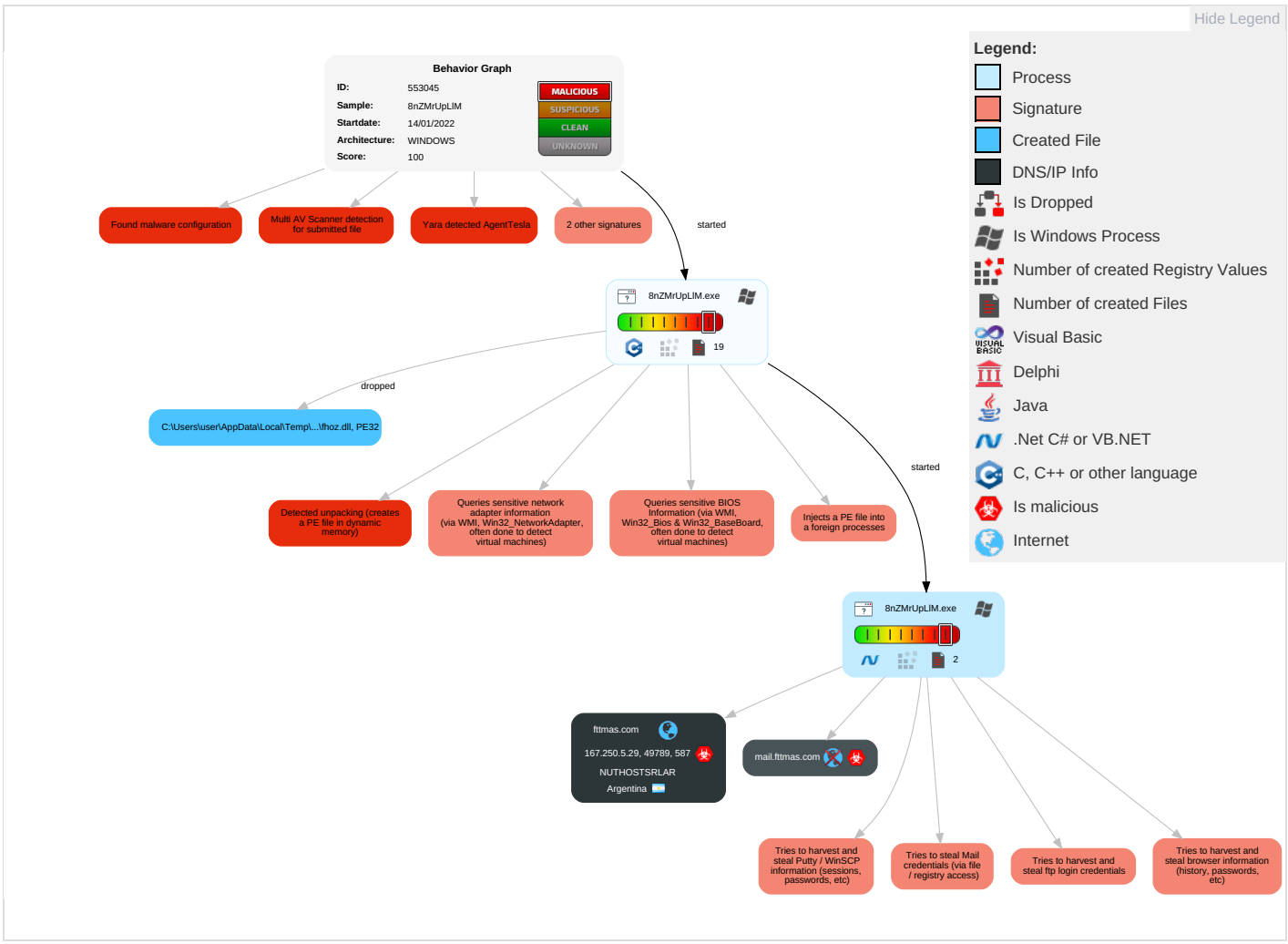
Remote Access Functionality:

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	Disable or Modify Tools 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	Deobfuscate/Decode Files or Information 1	Input Capture 1	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Credentials in Registry 1	System Information Discovery 1 2 7	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 3 1	LSA Secrets	Security Software Discovery 1 3 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 1 2	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	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

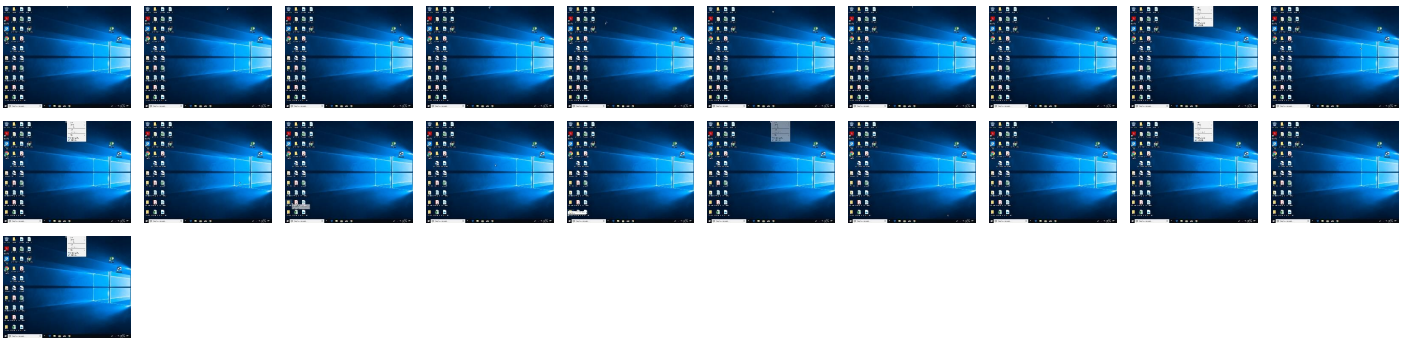
Behavior Graph



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
8nZMrUpLIM.exe	28%	Virustotal		Browse
8nZMrUpLIM.exe	28%	ReversingLabs	Win32.Trojan.Risis	
8nZMrUpLIM.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.8nZMrUpLIM.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.8nZMrUpLIM.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.1.8nZMrUpLIM.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.8nZMrUpLIM.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.8nZMrUpLIM.exe.400000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.8nZMrUpLIM.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.2.8nZMrUpLIM.exe.4980000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.8nZMrUpLIM.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.8nZMrUpLIM.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.0.8nZMrUpLIM.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://fttmas.com	0%	Virustotal		Browse
http://fttmas.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://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://sUJJ6pEBhL.org	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://dwAWQg.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	0%	URL Reputation	safe	
http://mail.fttmas.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
fttmas.com	167.250.5.29	true	true	• 0%, Virustotal, Browse	unknown
mail.fttmas.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
167.250.5.29	fttmas.com	Argentina		264649	NUTHOSTSRLAR	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553045
Start date:	14.01.2022
Start time:	07:41:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8nZMrUpLIM (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/4@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 26.3% (good quality ratio 24.5%) • Quality average: 78.4% • Quality standard deviation: 30.2%
HCA Information:	• Successful, ratio: 69% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
07:42:42	API Interceptor	743x Sleep call for process: 8nZMrUpLlM.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\ghlg3zknspvrw0ea2	
Process:	C:\Users\user\Desktop\8nZMrUpLlM.exe
File Type:	data
Category:	dropped
Size (bytes):	292863
Entropy (8bit):	7.961387462358669
Encrypted:	false
SSDEEP:	6144:IGXwC3PJz/7I+Y7Lqk+rtf5RBgsGxt37MPFi1SH7PC9aXmU0zHozYNd:v3R7W/2rZm5hCulTHKYNd

C:\Users\user\AppData\Local\Temp\ghlg3zknspvrw0ea2	
MD5:	8D64DA3B39791920EB7AE134B9A48148
SHA1:	F276A210B5223376E0DF20F08D756BAB90E32702
SHA-256:	07E9EC3F285DA6C383F61850C8D67E0F0B76F60630690397D4E1BFFE1FBD5CD1
SHA-512:	E9241352A47B0D38C6761B51B768408C855A08A20DC7713E896DD787626AD5B88248D429B4991643062A93967A34B956E2D7CD3CB276109E9CEF9EFAA7742ACD
Malicious:	false
Reputation:	low
Preview:	..zy.P..(j...I.l*Py.q..Qi.k% #..~=,lw....R.nZU.v.4.w.36c^.z..N'r.....s6~n8O.....C.-....6...o.;.I..Q-...u....4.P[.f,@..2..Vf...^.|.2*FH.....6..9.e..z.@^Q...u.H.8.(..A.....Q.@..''..W..C..g.: ...t..F'.h..*p?.JQ..aKi.....;Zq..Vy.f....9..0...U_.....l.5z..P.@.j.O...s.K.q..Qi..%,ty0V=,.w...;R.nZI.v.4.w.3Hc^.s....~.....6....DSBM.oI..I.P...7.....;.y..1.<V7O.....@`..2.2Vf....kT...2D. .x.R.TX#.VYsb..xp...I.j....I|.....t`>...&..j.....k.5...F..I.S2....S6[f@..I.Y..#W..%d..y.(3{h..Mnr.JU_.....D...P...j..I.XPy.q..Qi.k% #..~=.lw..\;@cnZ=.v.4iw.3.c^..z...~.....G.....oI... .P..7.).....s....<.7O..R...@Y....O.f....k7.....p...R..X~[.Ysb...p..sf..B...k[b..:.t ..C....j.....k.>.E.F..I.S2.HX..6[f@..I.Y..#f..hp..y.(3{h..Mnr.JU_.....I.5z..P.e(j..I.*Py.q..Qi.k% #..~=, lw....R.nZU.v.4.w.36c^.sz...~.....S.M.oI..d.P.t.7....;.s....<.7O..R...@`..2..Vf....kT.....px.R..X~[.Ysb..xp...I.j....I|.....t ...C.&..j.....k.5...F..I.S2.HX..6[f@..I.Y..#f..hp..

C:\Users\user\AppData\Local\Temp\nsd4888.tmp	
Process:	C:\Users\user\Desktop\8nZMrUpLlM.exe
File Type:	data
Category:	dropped
Size (bytes):	323487
Entropy (8bit):	7.816174377396866
Encrypted:	false
SSDEEP:	6144:qBvdGXwC3PJz/7I+Y7Lqk+rtf5RBgsGxt37MPFi1SH7PC9aXmU0zHozYN:MK3R7W/2rZm5hCulTHKYN
MD5:	5EB4915721C8C5A4CC54872E4EA45CB8
SHA1:	0CEE9BD6802E2156FAE97FB53C5F7092235002FC
SHA-256:	78E160318CC3F53E6DBA3A85B3D4586BBFD790D7198A62953950B39F93AA90F2
SHA-512:	C215F3BA4FDDE796DB75DE3500CF59EF520B080E143DB409BF9527E161BCCBBD9B5C5047F77DECEEB9BD2AA9FDA9632D75ADA848C05916909F70D8B72CCE 772
Malicious:	false
Reputation:	low
Preview:	.R.....,.....?.....Q.....R..... .....J.....j.....I..... ....

C:\Users\user\AppData\Local\Temp\nsd4889.tmp\fhoz.dll	
Process:	C:\Users\user\Desktop\8nZMrUpLlM.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	4.170385673760893
Encrypted:	false
SSDEEP:	48:SpowlUM6jb9EQlkuW2yH+ZsQMR7/iItlRuqSx:ZwG6eQFuoH+Zdc5xc
MD5:	D03EE97FCBFDCB10C041692ABC8F4B05
SHA1:	7324632CD1BE493042705D1EC15C2A0C318B268D
SHA-256:	44A5477EEA678326278FA1021A143D510FE4762880E295377609E98B8DE396A8
SHA-512:	5A82346B7A394235030FA5DBFCF6AAF1D34E017A3B4D490B3277503C9F287E190A748EA01F5E8C4C6D6F2F61197491F709CC1DDD7D2A8EBA43B94552B2C3EE 4
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x-2..Ca..Ca..CaZ.Ma..Ca..B`..Ca..Ba..Ca.lG`..Ca.lC`..Ca.l.a.. Ca.lA`..CaRich..Ca.....PE..L.....a.....!..... .....P.....@..... ..H....!.....0.....@..\..... .....text..... ..`.rdata..h.... .....@..@.rsrc.....0.....@..@.reloc..\....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\zxtswtId	
Process:	C:\Users\user\Desktop\8nZMrUpLlM.exe
File Type:	data
Category:	dropped
Size (bytes):	4793
Entropy (8bit):	6.193633641349719
Encrypted:	false
SSDEEP:	96:6eawFZzPD9U4NGzuU5ucjJAqMS1ONJ4mX9G59QPgbb2B7Y12WTvoqr:6elC+GzT5ucnMkON2a9GvQyaBMTroqr
MD5:	B574ABA6D4FAD0480F22BE4FB49CA6FE
SHA1:	05D6E3ED5F354154FE299AD0E9FEAA83A061A9D5
SHA-256:	8972CF1E3AD59A468E7A37E30F5EDF4AE2CFC90189B34E969394A6AEBBD41C79
SHA-512:	BFCA38663984CCEFB0A971C563F7912C16754E75FD6F013C4F489355DB6CA22B1766CB2589FDE561D242E5C2320515165C01A4A69AE23F5EC8306EA1C4A808C
Malicious:	false

C:\Users\user\AppData\Local\Temp\zxtswtId	
Reputation:	low
Preview:	...u;...@svw.%..w.&..E..w.&..E..%..E.....%..U..U.=E.p....9E.9u..U..U.=E.p....9E.9u..U..U.=E.p...9E.9u..U..U.=E.p.....9E.9u..M..V.Z.h[...E.)9E.9u.;E.....9E.9}.;E.;}.=....Z.i..;E.u.=..9E.wv9%....Z.....d...%..U.i.U.j.U.Ah.U.Ai.U.o.U.n..T.'x;..'x9|.`..U..U.Aj;E...9E.%.....Dd.c.....d..;%.no;E.onk;.m..u;.qq.w.&..E.;E.;..E.S`;E.;.;}.;..9u.;D..9E.;E.;.@;}.9.;E.;u .;.m..X...O.H....^.....X&..O.&....l.....X.l+O.t....z.....u;....w.&..E..E....=E.9E..M.T.;E...;E.@9E.;E.x9E.....TF;E.)Z.i[..9D..9t..=E.)Z.i...9D..9t..Z.Z.h[..=D..pX&..O...p.....9E..=E.p.U.. z...9E..M.T..%...E....;E.;.m..u;...@.w.&..E..E....=E.9E..M.T.;E...;E.@9E.;E.x9E...#.....:...;E.)Z.i[..9D..9t..;E.)Z.i...9D..9t..;E.)Z.i.9D..9t..;E...Z.j[.9D..9|..=E.)Z.i...9D..9t..Z.Z.h[.. =D..pX...O....p....9E..M..T.;E.;}.9...U..U..U..U.....9E..M.T..%...E....;E.;.m..u;....E....=E.9E..M.T.;E...;E.@9E.;E.x9E...Z.....TF;E.)Z.i[..9D..9t..;E.)Z.i...9D..9t..Z.Z.h[..=D. .pX.l+O.g...p.d...9E...U

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.937114283505084
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:	8nZMrUpLlM.exe
File size:	271273
MD5:	8d58419427c9169b0894ceee4659e905
SHA1:	e787266ae57b7e47c5151107f4e3d8c02a66c5bc
SHA256:	9661e4c97ebfc0a077645f7fc3ef0da1a98800400365fb86a2ac7a36767e7ba7
SHA512:	be2623f30f9f5ab3387417fa0560c98d1f5fb19fac163b90d71d7ae893056f92ebf438e7c70308940802f68793c8456de484a3f5c7c5b7087d086bbcb3e5a5f7
SSDEEP:	6144:owFb0GtyUN6m9Dkn+HmbUfoNmbXrJJ36Opv47sP9I5:p/tyU6mxk++UfoNWVh6uE0A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403225
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:	0x48EFCDC9 [Fri Oct 10 21:48:57 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:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5976	0x5a00	False	0.668619791667	data	6.46680044621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.444878472222	data	5.17796812871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55078125	data	4.68983486809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x900	0xa00	False	0.409375	data	3.94693169534	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

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 07:44:18.417675018 CET	192.168.2.5	8.8.8.8	0xa58e	Standard query (0)	mail.fttmas.com	A (IP address)	IN (0x0001)
Jan 14, 2022 07:44:18.457992077 CET	192.168.2.5	8.8.8.8	0xb6de	Standard query (0)	mail.fttmas.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 07:44:18.435215950 CET	8.8.8.8	192.168.2.5	0xa58e	No error (0)	mail.fttmas.com	fttmas.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 07:44:18.435215950 CET	8.8.8.8	192.168.2.5	0xa58e	No error (0)	fttmas.com		167.250.5.29	A (IP address)	IN (0x0001)
Jan 14, 2022 07:44:18.494725943 CET	8.8.8.8	192.168.2.5	0xb6de	No error (0)	mail.fttmas.com	fttmas.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 07:44:18.494725943 CET	8.8.8.8	192.168.2.5	0xb6de	No error (0)	fttmas.com		167.250.5.29	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2022 07:44:19.571890116 CET	587	49789	167.250.5.29	192.168.2.5	220-taho.servidoraweb.net ESMTP Exim 4.94.2 #2 Fri, 14 Jan 2022 03:44:24 -0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 14, 2022 07:44:19.575205088 CET	49789	587	192.168.2.5	167.250.5.29	EHLO 445817
Jan 14, 2022 07:44:19.812509060 CET	587	49789	167.250.5.29	192.168.2.5	250-taho.servidoraweb.net Hello 445817 [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 07:44:19.813898087 CET	49789	587	192.168.2.5	167.250.5.29	STARTTLS
Jan 14, 2022 07:44:20.055238008 CET	587	49789	167.250.5.29	192.168.2.5	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 8nZMrUpLIM.exe PID: 1056 Parent PID: 5732

General

Start time:	07:42:28
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\8nZMrUpLIM.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\8nZMrUpLIM.exe"
Imagebase:	0x400000
File size:	271273 bytes
MD5 hash:	8D58419427C9169B0894CEEE4659E905
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: 00000001.00000002.248124779.0000000003040000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.248124779.0000000003040000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: 8nZMrUpLlM.exe PID: 4380 Parent PID: 1056

General

Start time:	07:42:29
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\8nZMrUpLlM.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\8nZMrUpLlM.exe"
Imagebase:	0x400000
File size:	271273 bytes
MD5 hash:	8D58419427C9169B0894CEEE4659E905
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: 00000002.00000002.502323275.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.502323275.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.507139784.0000000004982000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.507139784.0000000004982000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.246842108.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.246842108.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000001.247299670.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000001.247299670.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.503896589.0000000000694000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.503896589.0000000000694000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.505385484.000000000B60000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.505385484.000000000B60000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.506959531.00000000034A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.506959531.00000000034A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.245307233.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.245307233.0000000000414000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.505801897.00000000024A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.505801897.00000000024A1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis