ID: 383921
Sample Name: mal5.exe
Cookbook: default.jbs
Time: 12:29:27
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

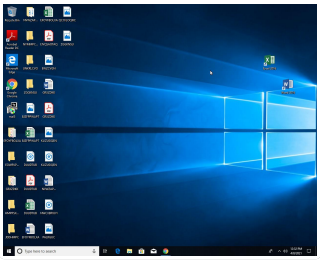
Analysis Report mal5.exe

Overview

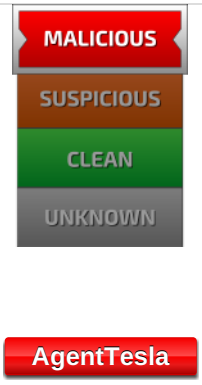
General Information

Sample Name:	mal5.exe
Analysis ID:	383921
MD5:	082b50aa4a4cca..
SHA1:	d6fb2b9d96280dd.
SHA256:	6ed8f5c23004500.
Infos:	

Most interesting Screenshot:



Detection



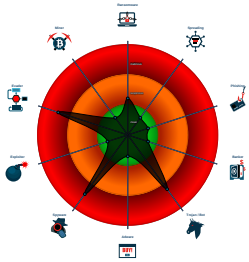
AgentTesla

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Contains functionality to prevent loc…
- Maps a DLL or memory area into an…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…
- Tries to harvest and steal ftp login c…
- Tries to steal Mail credentials (via fil…
- Antivirus or Machine Learning detec…
- Contains capabilities to detect virtua…

Classification



Startup

- **System is w10x64**
- mal5.exe (PID: 400 cmdline: 'C:\Users\user\Desktop\mal5.exe' MD5: 082B50AA4A4CCAEA6B415DE2E968AD47)
  - mal5.exe (PID: 4672 cmdline: 'C:\Users\user\Desktop\mal5.exe' MD5: 082B50AA4A4CCAEA6B415DE2E968AD47)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "vladmir@mail.commarcellinussmtp.mail.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000001.235962942.000000000041 4000.00000040.00020000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.240515409.000000001ED8 0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: mal5.exe PID: 400	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: mal5.exe PID: 4672	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

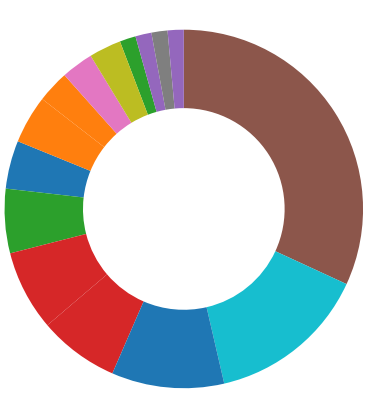
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.mal5.exe.1ed91458.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.mal5.exe.1ed80000.5.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.1.mal5.exe.415058.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.1.mal5.exe.415058.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.1.mal5.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 2 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- 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:

Found malware configuration

Multi AV Scanner detection for submitted file

Malware Analysis System Evasion:

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)

HIPS / PFW / Operating System Protection Evasion:

Contains functionality to prevent local Windows debugging

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

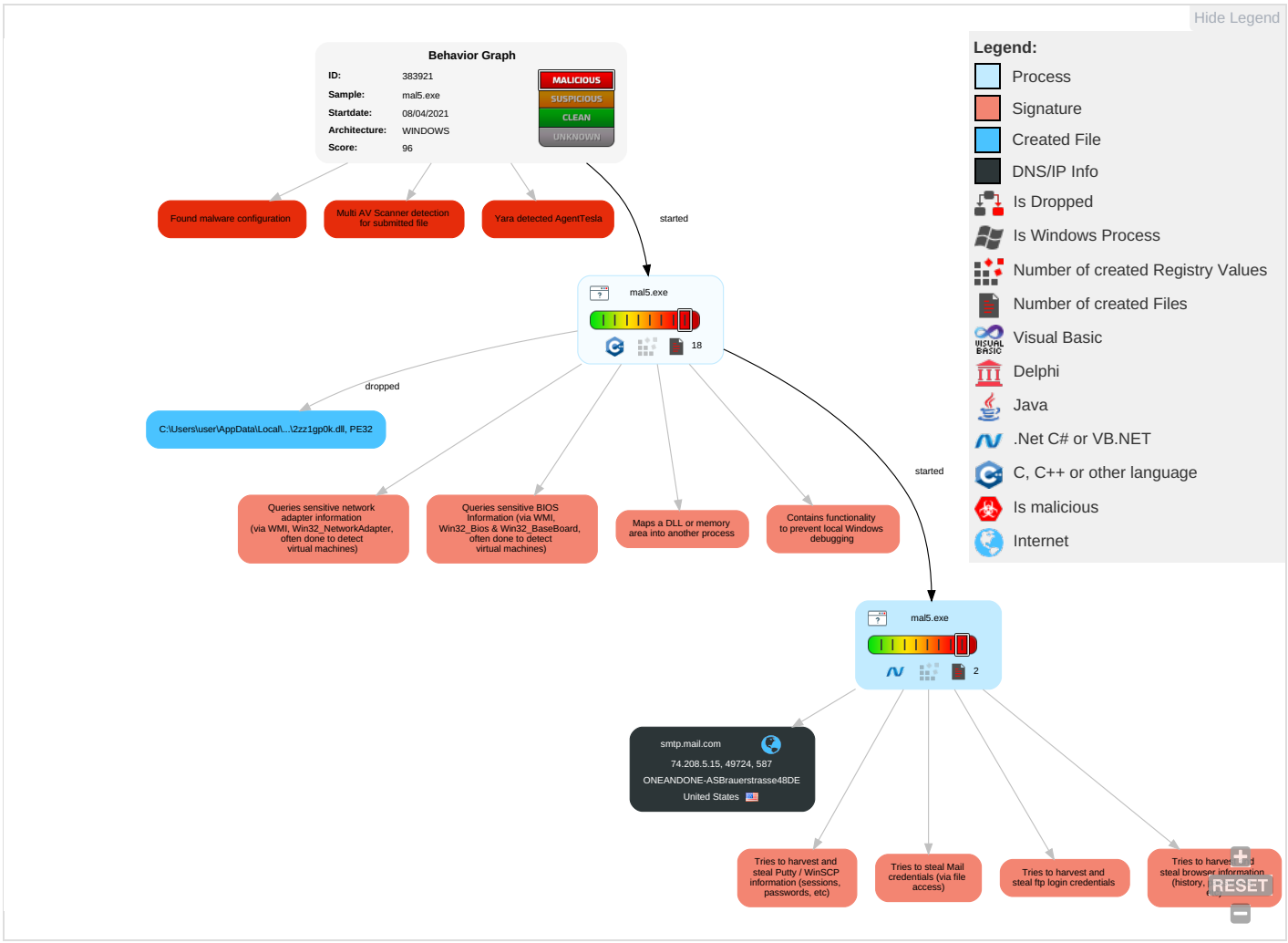
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 2 1 1	Disable or Modify Tools 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 1	Credentials in Registry 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)	Software Packing 1	Security Account Manager	System Information Discovery 1 2 6	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 1 4 1	NTDS	Query Registry 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 2 1 1	LSA Secrets	Security Software Discovery 1 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Process Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Virtualization/Sandbox Evasion 1 4 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
mal5.exe	32%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.mal5.exe.73360000.6.unpack	100%	Avira	HEUR/AGEN.1131513		Download File
1.1.mal5.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.mail.com	74.208.5.15	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	mal5.exe	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
74.208.5.15	smtp.mail.com	United States		8560	ONEANDONE-ASBrauerstrasse48DE	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383921
Start date:	08.04.2021

Start time:	12:29:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	mal5.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:	27
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:	mal96.troj.spyw.evad.winEXE@3/3@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 69.7% (good quality ratio 64.5%) • Quality average: 77.5% • Quality standard deviation: 30.7%
HCA Information:	• Successful, ratio: 68% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 168.61.161.212, 40.88.32.150, 95.100.54.203, 104.43.139.144, 13.107.42.23, 13.107.5.88, 20.82.209.104, 23.10.249.26, 23.10.249.43, 20.82.209.183, 20.50.102.62, 20.54.26.129, 23.54.113.53, 52.155.217.156 • Excluded domains from analysis (whitelisted): client-office365-tas.msedge.net, ocos-office365-s2s.msedge.net, arc.msn.com.nsatc.net, config.edge.skype.com.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, l-0014.config.skype.com, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, config.edge.skype.com, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, afdo-tas-offload.trafficmanager.net, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, l-0014.l-msedge.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:30:31	API Interceptor	832x Sleep call for process: mal5.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
74.208.5.15	Order 100955-21042021.exe	Get hash	malicious	Browse	
	ORDER 100955-21042021.exe	Get hash	malicious	Browse	
	Price request.exe	Get hash	malicious	Browse	
	gzOWUFf99a.exe	Get hash	malicious	Browse	
	pB5deM6Hti.exe	Get hash	malicious	Browse	
	mVxZxsQdkU.exe	Get hash	malicious	Browse	
	Shipping Documents_Original BL, Invoice & Packing List.exe	Get hash	malicious	Browse	
	2021-102899.exe	Get hash	malicious	Browse	
	Scan_23748991000.exe	Get hash	malicious	Browse	
	KI2011-2982..exe	Get hash	malicious	Browse	
	PO-87655.exe	Get hash	malicious	Browse	
	Document pdf .exe	Get hash	malicious	Browse	
	Document pdf.....exe	Get hash	malicious	Browse	
	mvl9cPORxx.exe	Get hash	malicious	Browse	
	9MwNPG0Fqx.exe	Get hash	malicious	Browse	
	PO 304161.exe	Get hash	malicious	Browse	
	okurtrte.exe	Get hash	malicious	Browse	
	j5C4kIKEckYxsyY.exe	Get hash	malicious	Browse	
	new order.exe	Get hash	malicious	Browse	
	DHL-AWB.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.mail.com	Order 100955-21042021.exe	Get hash	malicious	Browse	• 74.208.5.15
	ORDER 100955-21042021.exe	Get hash	malicious	Browse	• 74.208.5.15
	RFQ.scr.exe	Get hash	malicious	Browse	• 74.208.5.15
	Price request.exe	Get hash	malicious	Browse	• 74.208.5.15
	SecuriteInfo.com.Trojan.Win32.Save.a.29235.exe	Get hash	malicious	Browse	• 74.208.5.15
	gzOWUFf99a.exe	Get hash	malicious	Browse	• 74.208.5.15
	pB5deM6Hti.exe	Get hash	malicious	Browse	• 74.208.5.15
	mVxZxsQdkU.exe	Get hash	malicious	Browse	• 74.208.5.15
	Shipping Documents_Original BL, Invoice & Packing List.exe	Get hash	malicious	Browse	• 74.208.5.15
	2021-102899.exe	Get hash	malicious	Browse	• 74.208.5.15
	Scan_23748991000.exe	Get hash	malicious	Browse	• 74.208.5.15
	KI2011-2982..exe	Get hash	malicious	Browse	• 74.208.5.15
	PO-87655.exe	Get hash	malicious	Browse	• 74.208.5.15
	Document pdf .exe	Get hash	malicious	Browse	• 74.208.5.15
	Document pdf.....exe	Get hash	malicious	Browse	• 74.208.5.15
	mvl9cPORxx.exe	Get hash	malicious	Browse	• 74.208.5.15
	9MwNPG0Fqx.exe	Get hash	malicious	Browse	• 74.208.5.15
	PO 304161.exe	Get hash	malicious	Browse	• 74.208.5.15
	okurtrte.exe	Get hash	malicious	Browse	• 74.208.5.15
	j5C4kIKEckYxsyY.exe	Get hash	malicious	Browse	• 74.208.5.15

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ONEANDONE-ASBrauerstrasse48DE	invoice.exe	Get hash	malicious	Browse	• 74.208.236.64
	PO7321.exe	Get hash	malicious	Browse	• 217.160.0.101
	BL01345678053567.exe	Get hash	malicious	Browse	• 74.208.236.134
	A409043090.exe	Get hash	malicious	Browse	• 74.208.5.2
	Old9BZy7jO.dll	Get hash	malicious	Browse	• 82.223.21.211
	mULT14gGmy.dll	Get hash	malicious	Browse	• 82.223.21.211
	yWA1Ay0538.dll	Get hash	malicious	Browse	• 82.223.21.211
	27XuTqKwYF.dll	Get hash	malicious	Browse	• 82.223.21.211
	Old9BZy7jO.dll	Get hash	malicious	Browse	• 82.223.21.211
	mULT14gGmy.dll	Get hash	malicious	Browse	• 82.223.21.211
	JI63JG7EMo.dll	Get hash	malicious	Browse	• 82.223.21.211
	F7aZDNx6UM.dll	Get hash	malicious	Browse	• 82.223.21.211
	yWA1Ay0538.dll	Get hash	malicious	Browse	• 82.223.21.211
	27XuTqKwYF.dll	Get hash	malicious	Browse	• 82.223.21.211
	NYDhNBQlYM.dll	Get hash	malicious	Browse	• 82.223.21.211
	ydKCqL4sTG.dll	Get hash	malicious	Browse	• 82.223.21.211

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	F7aZDNx6UM.dll	Get hash	malicious	Browse	• 82.223.21.211
	JI63JG7EMo.dll	Get hash	malicious	Browse	• 82.223.21.211
	TI8E08zJuu.dll	Get hash	malicious	Browse	• 82.223.21.211
	NYDhNBQlYM.dll	Get hash	malicious	Browse	• 82.223.21.211

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\627zxnx9ige	
Process:	C:\Users\user\Desktop\mal5.exe
File Type:	data
Category:	dropped
Size (bytes):	12805
Entropy (8bit):	7.960326474428052
Encrypted:	false
SSDEEP:	192:x6mdiWh0YXB8zkV1FI3N3fkd9H351UiWq6DzhCwVOaeKQdtTs9lC/oCRwoBn:xd5Fkk63Cd9XjdW5zhCwVO9YMwCZ
MD5:	BA407134296ACA1A76B2445EC07FACE6
SHA1:	46EFA417A7C1F97725E9E885EC06F83079717070
SHA-256:	E912FA0B3EC39A5DE5BC87B02CA52536D87BAC9FD15BFF462DF4543F83207658
SHA-512:	B3DE16B800E50C131865135E6ED665CC6ACF529D19AB6067D1E4C4776EBD9434948002D13DC233E4A6720378876FF3EABEE56C7133795A029AED519686D1272
Malicious:	false
Reputation:	low
Preview:	,5.!_M.#.....C.3.....q...^.....8e..5..R.k.....1M....O...Z.,m.l..RKO.....]...~.4.S..546.h....T...e...J..$.-._....;...l."..@.#.(.Z..u..*.K....'f.W..=}.l..}.l:.....]....N[S..p.U1..W..T..v....J.,1 ..X.....cP.X.X...RN#.....;.....7...E..t?M..C.}...F..B.;...-.5.-..k./Ye)f"..e.F..X..J.Yz..TP}...{.-k..3r?q..Sx8...Q.$b.?.{.1-X..6.;.m.7..Y.-.j. ;O..!~*.\.-..@.$.a..!.E.(.).[.#z.....P.... ,k..C."a.C..I....$#b.....Xy.....p'.H.I.....OP..%gC..j..j..<...3O..Vj4q...(....;{.I...f...b?..t.....$c..x.....X..IJ...:..J*.yF..c.D"..7Te...@x._.8....0i.p....^).v...~.....\.b.....w.S.v#..X..J.. =>}b..b#...c.!f...e.vox...{..@d.wY.U..`...cs..b...^..".F..{A..tD..v..].Q.X....l..>.V.F..1fa...OM..AC...i.Ue...)..6.`.NPa....."..]..g{ja...M.^..Fxa...T.._..cW..+U.. (h.O..A.... ..@.h!..%..@". 0=]r.QP....J..Jj..ue. ..3..S.T...C...X..].r...S.|..=..Y.h..-..=.Z.I..;;...z.;zd....].@.....7{.t..g....v.@.w."a...G.~.g0.#b.l..JXR.m...~.....I.....x-.h.E&..l.s.. ...5q...,.)..."

C:\Users\user\AppData\Local\Temp\nsaC339.tmp\2zz1gp0k.dll	
Process:	C:\Users\user\Desktop\mal5.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.1424095849549705
Encrypted:	false
SSDEEP:	48:StkZ7LwJeaowJ5PHhqu8MUEm17OGa4zzBvoAXAdUMQ9BgqRuqS:HKearyZUGXHBgVueKx
MD5:	D043386FA2E6761571E3C595B890D147
SHA1:	7C8E0692709155338 70A787C360522B9518376E3
SHA-256:	A778BFDA899CC4DB43CAF917D13C4A29313B2180EA445C97D35D9A9DE9225943
SHA-512:	61C658BDA73BEFB90AFA4D7661A714F91B2B448C173174B9924D4F2037BCB6BD864EF3BBFB21686E9F4B58BAA57A2DC3DFD10B05FB641417AA735E77EAA3E5 C9
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;T..hT..hT..h@..iG..hT..h{..h...iU..h...iU..h...hU..h...iU..hRichT..h. .....PE..L....bn`.....!..... ..... .....`.....@..... !..T...`".....@.....P..p....!..... ..... .....text..... ..`.rdata..0.... .....@..@.data.....0.....@....rsrc.....@.....@..@.reloc..p....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\x1y8d3vne767i3k	
Process:	C:\Users\user\Desktop\mal5.exe
File Type:	data
Category:	dropped
Size (bytes):	292864
Entropy (8bit):	**7.9994745566549454**
Encrypted:	**true**

C:\Users\user\AppData\Local\Temp\x1y8d3vne767i3k	
SSDEEP:	6144:NmxzkJx9Ang+vi0VS4x7bpqkR6Ay4fqPw6snuyhGEnLq7W6QQq0+fyLH:Nd9K1viqrx7Nj4r4fcpFyhGm5gqfyL
MD5:	68ECE93FFAAE453D36BE3B07C3EF4782
SHA1:	C95B73F4A00C007D3CD60FB1EB876AB6BB782564
SHA-256:	9B72538EE33A2936D929F9560740D98C803883631C81382DAC5DB79987AEBDEA
SHA-512:	B95B15326D7C876456316C2AD488B9FF86346454A32EAB2CBBB622D960A683C418B86AF6329D10765D76941D63B20001C660BA0EB1246397D0168B1EE3D52089
Malicious:	false
Reputation:	low
Preview:	...ru..).x.\;.....{<.HU..4....o.k.C....ZdSN...*.K....<Z..G.(...`f31.1u..U.y ...`....>.b..XG...`Wl.X..ryI.....mI.2.....x:..7.D...da.f)...&..n\.B.....L..>e.....b L%....%...Q.c..... ...e.V_.M.$pV.q..Q..n.@.y..*u.z5 I..e2[V..\..9@{.....Q.....t...k+.,.\.1.jG4...7{1.....S/~.....i.g..z....!`....;VGa...2.....Q.k.$.uJ."....:.?..w.mF\....H..I..."..|.6....vLS-+.....`..X...r 8r..eu.+....K..^C.o.4'.....Bf.S*..q....y...G..Ll....XI.g.{..L.$.rE.....bW.A`.Xi..O..s+Z..2}....CC...?.|<.i...B....vz.....w..>..N....f.y.G{dJgk9..AR..AA.7.&P.....S.?.t.d..av.+o..... .]...A7>{.~-....+]..<.....Z..fr%...tO.....mM..5.+M....t....>&>.jay.b..Y.....c.u.....,.Y..;'.....|.C:..,`.[]MxG..B>5.G.....uo..f.a...Y(b(...OHEi...Z...}..P.M..@]^\#.p:.L3...o..._F.6....c fOk.Y.n..T.[$:.....&....^.*....u.T.'6.....`....].w.Qx.OZ....C.o,...V....].=.k.F.#....!#e...D....(.eLo.Fh5...S$!.E.,..N...:.w...Y...G.sg....`GQP....mY....._c{:.J..Bd..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.956646648444615
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:	mal5.exe
File size:	340902
MD5:	082b50aa4a4ccaea6b415de2e968ad47
SHA1:	d6fb2b9d96280dd812325fe8338f646dd918cfdb
SHA256:	6ed8f5c23004500f4125edd751c5129935bb62a182d5922b1108fb618bf45961
SHA512:	68c03e42a17224d69bafed16d3d1bb32256480db06cc8ac79280898c6bd0196abea72b16f71d75c670a245b408b61f60dab9dd2edc1c72fa2e3e43174f4da5ba
SSDEEP:	6144:HdRgoHmxzkJx9Ang+vi0VS4x7bpqkR6Ay4fqPw6snuyhGEnLq7W6QQq0+fyLRvW:jPd9K1viqrx7Nj4r4fcpFyhGm5gqfy0
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.H..... .....,.....:...!.....&.....e.....Rich.....PE..L..... 8E.....Z....9.....J1.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40314a
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:	0x4538CD0B [Fri Oct 20 13:20:11 2006 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0

General

File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	18bc6fa81e19f21156316b1ae696ed6b

Entrypoint Preview

Instruction
sub esp, 0000017Ch
push ebx
push ebp
push esi
xor esi, esi
push edi
mov dword ptr [esp+18h], esi
mov ebp, 00409240h
mov byte ptr [esp+10h], 00000020h
call dword ptr [00407030h]
push esi
call dword ptr [00407270h]
mov dword ptr [007A3030h], eax
push esi
lea eax, dword ptr [esp+30h]
push 00000160h
push eax
push esi
push 0079E540h
call dword ptr [00407158h]
push 00409230h
push 007A2780h
call 00007F640CA9D8C8h
mov ebx, 007AA400h
push ebx
push 00000400h
call dword ptr [004070B4h]
call 00007F640CA9B009h
test eax, eax
jne 00007F640CA9B0C6h
push 000003FBh
push ebx
call dword ptr [004070B0h]
push 00409228h
push ebx
call 00007F640CA9D8B3h
call 00007F640CA9AFE9h
test eax, eax
je 00007F640CA9B1E2h
mov edi, 007A9000h
push edi
call dword ptr [00407140h]
call dword ptr [004070ACh]
push eax
push edi
call 00007F640CA9D871h
push 00000000h
call dword ptr [00407108h]
cmp byte ptr [007A9000h], 00000022h
mov dword ptr [007A2F80h], eax
mov eax, edi
jne 00007F640CA9B0ACh
mov byte ptr [esp+10h], 00000022h
mov eax, 00000001h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7344	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3ac000	0x900	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x280	.rdata
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	0x59de	0x5a00	False	0.681293402778	data	6.5143386598	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x10f2	0x1200	False	0.430338541667	data	5.0554281206	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x39a034	0x400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a4000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3ac000	0x900	0xa00	False	0.409375	data	3.94574916515	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3ac190	0x2e8	data	English	United States
RT_DIALOG	0x3ac478	0x100	data	English	United States
RT_DIALOG	0x3ac578	0x11c	data	English	United States
RT_DIALOG	0x3ac698	0x60	data	English	United States
RT_GROUP_ICON	0x3ac6f8	0x14	data	English	United States
RT_MANIFEST	0x3ac710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	CloseHandle, SetFileTime, CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetFileSize, GetModuleFileNameA, GetTickCount, GetCurrentProcess, lstrcmpiA, ExitProcess, GetCommandLineA, GetWindowsDirectoryA, GetTempPathA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, lstrcmpA, GetEnvironmentVariableA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, SetErrorMode, GetModuleHandleA, LoadLibraryA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, CopyFileA
USER32.dll	ScreenToClient, GetWindowRect, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, EndDialog, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxA, CharPrevA, DispatchMessageA, PeekMessageA, CreateDialogParamA, DestroyWindow, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, TrackPopupMenu, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow

DLL	Import
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetMalloc, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 54

- 53 (DNS)
- 587 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:32:01.822705984 CEST	49724	587	192.168.2.5	74.208.5.15
Apr 8, 2021 12:32:01.957596064 CEST	587	49724	74.208.5.15	192.168.2.5
Apr 8, 2021 12:32:01.957729101 CEST	49724	587	192.168.2.5	74.208.5.15
Apr 8, 2021 12:32:02.092514038 CEST	587	49724	74.208.5.15	192.168.2.5
Apr 8, 2021 12:32:02.101658106 CEST	49724	587	192.168.2.5	74.208.5.15
Apr 8, 2021 12:32:02.234574080 CEST	587	49724	74.208.5.15	192.168.2.5
Apr 8, 2021 12:32:02.234661102 CEST	587	49724	74.208.5.15	192.168.2.5
Apr 8, 2021 12:32:02.264161110 CEST	49724	587	192.168.2.5	74.208.5.15
Apr 8, 2021 12:32:02.397782087 CEST	587	49724	74.208.5.15	192.168.2.5
Apr 8, 2021 12:32:02.452738047 CEST	49724	587	192.168.2.5	74.208.5.15
Apr 8, 2021 12:32:03.442888975 CEST	49724	587	192.168.2.5	74.208.5.15
Apr 8, 2021 12:32:03.578908920 CEST	587	49724	74.208.5.15	192.168.2.5
Apr 8, 2021 12:32:03.578946114 CEST	587	49724	74.208.5.15	192.168.2.5
Apr 8, 2021 12:32:03.579061985 CEST	49724	587	192.168.2.5	74.208.5.15
Apr 8, 2021 12:32:03.579154968 CEST	587	49724	74.208.5.15	192.168.2.5
Apr 8, 2021 12:32:03.584762096 CEST	49724	587	192.168.2.5	74.208.5.15
Apr 8, 2021 12:32:03.717971087 CEST	587	49724	74.208.5.15	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:32:03.843502045 CEST	49724	587	192.168.2.5	74.208.5.15
Apr 8, 2021 12:32:03.960912943 CEST	49724	587	192.168.2.5	74.208.5.15
Apr 8, 2021 12:32:04.094665051 CEST	587	49724	74.208.5.15	192.168.2.5
Apr 8, 2021 12:32:04.097685099 CEST	49724	587	192.168.2.5	74.208.5.15
Apr 8, 2021 12:32:04.230468035 CEST	587	49724	74.208.5.15	192.168.2.5
Apr 8, 2021 12:32:04.231508970 CEST	49724	587	192.168.2.5	74.208.5.15
Apr 8, 2021 12:32:04.406544924 CEST	587	49724	74.208.5.15	192.168.2.5
Apr 8, 2021 12:32:04.695693970 CEST	587	49724	74.208.5.15	192.168.2.5
Apr 8, 2021 12:32:04.696547985 CEST	49724	587	192.168.2.5	74.208.5.15
Apr 8, 2021 12:32:04.830377102 CEST	587	49724	74.208.5.15	192.168.2.5
Apr 8, 2021 12:32:04.832437992 CEST	587	49724	74.208.5.15	192.168.2.5
Apr 8, 2021 12:32:04.835131884 CEST	49724	587	192.168.2.5	74.208.5.15
Apr 8, 2021 12:32:04.969739914 CEST	587	49724	74.208.5.15	192.168.2.5
Apr 8, 2021 12:32:05.046675920 CEST	49724	587	192.168.2.5	74.208.5.15
Apr 8, 2021 12:32:05.111852884 CEST	49724	587	192.168.2.5	74.208.5.15
Apr 8, 2021 12:32:05.247267008 CEST	587	49724	74.208.5.15	192.168.2.5
Apr 8, 2021 12:32:05.247291088 CEST	587	49724	74.208.5.15	192.168.2.5
Apr 8, 2021 12:32:05.247364044 CEST	49724	587	192.168.2.5	74.208.5.15
Apr 8, 2021 12:32:05.247420073 CEST	49724	587	192.168.2.5	74.208.5.15

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:30:11.758429050 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:30:11.773458958 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 8, 2021 12:30:21.379439116 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:30:21.391278028 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 8, 2021 12:30:23.997577906 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:30:24.011401892 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 8, 2021 12:30:24.837567091 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:30:24.850387096 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 8, 2021 12:30:25.712301970 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:30:25.726860046 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 8, 2021 12:30:26.486350060 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:30:26.501661062 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 8, 2021 12:30:34.134902954 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:30:34.148612976 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 8, 2021 12:30:34.936539888 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:30:34.949727058 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 8, 2021 12:30:37.701077938 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:30:37.718965054 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 8, 2021 12:30:37.925169945 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:30:37.937561989 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 8, 2021 12:30:39.374067068 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:30:39.386559963 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 8, 2021 12:30:39.694572926 CEST	59736	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:30:39.694892883 CEST	51058	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:30:39.697204113 CEST	52636	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:30:39.706667900 CEST	53	51058	8.8.8.8	192.168.2.5
Apr 8, 2021 12:30:39.706861019 CEST	53	59736	8.8.8.8	192.168.2.5
Apr 8, 2021 12:30:39.710190058 CEST	53	52636	8.8.8.8	192.168.2.5
Apr 8, 2021 12:30:40.209628105 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:30:40.222141027 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 8, 2021 12:30:40.890858889 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:30:40.904078960 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 8, 2021 12:30:42.880877018 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:30:42.906075954 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 8, 2021 12:30:47.945589066 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:30:47.963464022 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 8, 2021 12:31:18.805118084 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:31:18.837907076 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 8, 2021 12:31:22.476434946 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:31:22.496023893 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 8, 2021 12:31:54.651629925 CEST	64345	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:31:54.665647030 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 8, 2021 12:32:01.640417099 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:32:01.653584003 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 8, 2021 12:32:06.567998886 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:32:06.602636099 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 8, 2021 12:32:07.760463953 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:32:07.778455019 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 8, 2021 12:32:43.022455931 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:32:43.034904003 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 8, 2021 12:32:43.256335974 CEST	58530	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:32:43.282418013 CEST	53	58530	8.8.8.8	192.168.2.5
Apr 8, 2021 12:32:52.632229090 CEST	53813	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:32:52.645483971 CEST	53	53813	8.8.8.8	192.168.2.5
Apr 8, 2021 12:32:53.342799902 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:32:53.356025934 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 8, 2021 12:32:53.894257069 CEST	57344	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:32:53.907363892 CEST	53	57344	8.8.8.8	192.168.2.5
Apr 8, 2021 12:32:55.185738087 CEST	54450	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:32:55.198589087 CEST	53	54450	8.8.8.8	192.168.2.5
Apr 8, 2021 12:32:55.616451025 CEST	59261	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:32:55.629837990 CEST	53	59261	8.8.8.8	192.168.2.5
Apr 8, 2021 12:32:56.066224098 CEST	57151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:32:56.079045057 CEST	53	57151	8.8.8.8	192.168.2.5
Apr 8, 2021 12:32:56.480528116 CEST	59413	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:32:56.493791103 CEST	53	59413	8.8.8.8	192.168.2.5
Apr 8, 2021 12:32:57.098135948 CEST	60516	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:32:57.111306906 CEST	53	60516	8.8.8.8	192.168.2.5
Apr 8, 2021 12:32:57.878212929 CEST	51649	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:32:57.890654087 CEST	53	51649	8.8.8.8	192.168.2.5
Apr 8, 2021 12:32:58.233624935 CEST	65086	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:32:58.249414921 CEST	53	65086	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 12:32:01.640417099 CEST	192.168.2.5	8.8.8.8	0x1ab5	Standard query (0)	smtp.mail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 12:32:01.653584003 CEST	8.8.8.8	192.168.2.5	0x1ab5	No error (0)	smtp.mail.com		74.208.5.15	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 8, 2021 12:32:02.092514038 CEST	587	49724	74.208.5.15	192.168.2.5	220 mail.com (mrgmxus005) Nemesis ESMTP Service ready
Apr 8, 2021 12:32:02.101658106 CEST	49724	587	192.168.2.5	74.208.5.15	EHLO 579569
Apr 8, 2021 12:32:02.234661102 CEST	587	49724	74.208.5.15	192.168.2.5	250-mail.com Hello 579569 [185.32.222.8] 250-8BITMIME 250-AUTH LOGIN PLAIN 250-SIZE 141557760 250 STARTTLS
Apr 8, 2021 12:32:02.264161110 CEST	49724	587	192.168.2.5	74.208.5.15	STARTTLS
Apr 8, 2021 12:32:02.397782087 CEST	587	49724	74.208.5.15	192.168.2.5	220 OK

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: mal5.exe PID: 400 Parent PID: 5552

General

Start time:	12:30:19
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\mal5.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\mal5.exe'
Imagebase:	0x400000
File size:	340902 bytes
MD5 hash:	082B50AA4A4CCAEA6B415DE2E968AD47
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: 00000000.00000002.240515409.000000001ED80000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40313D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsfC309.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\627zxnx9ige	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\x1y8d3vne767i3k	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\nsaC339.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
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	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsaC339.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsaC339.tmp\2zz1gp0k.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsfC309.tmp	success or wait	1	4031E6	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsaC339.tmp	success or wait	1	405325	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\627zxnx9ige	unknown	12805	2c 35 9f 21 5f 4d fc 23 04 bc 88 15 f3 43 d5 33 fb 8d c7 f8 cf e9 71 0b d6 82 c1 5e f0 82 b0 dd ed 8d 19 a9 38 65 94 a4 35 bc b8 52 dc 6b 0a b2 db e0 8d cd da b1 b7 a9 31 4d 87 cb 09 a9 4f fd 16 da 5a db 97 2c 6d e3 6c ab ea 52 4b 4f 0b a1 b9 d5 e0 1f 5d c1 95 c0 7e f1 34 c7 53 92 d1 35 34 36 f2 68 aa bb d7 16 54 ac 01 b9 65 da 1b bf 4a 89 c8 24 df 2d e1 5f 9b b1 be fd 3b 9f 9c a2 6c e3 22 b3 01 40 7f 23 db 28 e0 5a 94 a7 75 b4 f2 8e 2a 97 4b c8 01 9b e8 27 66 06 57 0b c7 3d 7d 9d 6c ab e9 7d fd 6c 3a b5 f0 7f df 1e 5d f1 b4 fa b6 0c 4e 5b 53 92 d0 70 f4 55 31 86 c7 57 d6 15 54 86 7f 76 cc 0c 1a 0b 4a 89 2c 31 2e ea 58 a8 15 dc a1 e5 99 17 63 50 97 58 9b 58 ce 1e 8b 52 4e 23 0f 84 d5 c2 0d 87 0f c7 3b 8b 08 c1 86 ca 86 fc 0e 37 88 07 86 45 b7 cb 74 3f 4d	,5.!_M.#.....C.3.....q....^.. .....8e..5..R.k.....1M.. ..O...Z..,m.l..RKO.....]...~. 4.S..546.h....T...e...J..$.-._ ....;...l."..@.#.(.Z..u...*.K. ...'f.W..=}.I..}.l:.....]..... N[S..p.U1..W..T..v....J.,1..X .....cP.X.X...RN#.....;... .....7...E..t?M	success or wait	1	403017	WriteFile
C:\Users\user\AppData\Local\Temp\x1y8d3vne767i3k	unknown	32768	e0 1f f0 72 75 a7 ca 29 a7 78 18 5c 3b 92 0e bb b3 bf 8d e4 09 7b 3c bb 48 55 85 eb 34 af d2 e3 0a 6f ad 6b d8 43 02 87 cb b4 c4 5a 64 53 4e f2 da 93 c8 2a 0c 4b b8 ef d1 19 3c 5a e5 a7 d3 80 47 09 28 82 e4 15 60 66 33 31 a9 31 75 82 ed 55 ef 79 20 a0 bb ec 60 b1 cf 83 bb 83 3e 81 62 99 e0 b2 58 47 10 ce 9f 01 60 57 6c f1 58 9b 19 72 79 49 eb f1 89 01 a6 f2 11 99 ac 6d 49 11 32 f6 00 fa d8 b2 b1 b0 93 ad 78 3a 95 0a 37 1c 44 c8 9f e1 e0 64 61 c1 66 29 a4 f5 f6 26 a2 80 6e 5c c4 42 c5 b0 15 9b ae c7 d4 4c d8 cf 3e 65 19 dc f8 c1 a6 05 b0 a5 fc cf cb a5 a4 a5 81 e8 81 d9 62 20 4c 25 83 b6 17 da 25 ea c5 ed 51 b9 63 d7 89 f9 a8 bc fe ac 1a ee e8 65 bb 56 5f ff 4d 1f 24 70 56 82 71 a3 f9 51 94 dc 6e 03 40 aa 79 9b 0c 2a 75 07 7a 35 20 6c 15 e5 65 32 5b 56 ad	...ru..).x.\;.....{<.HU..4. ...o.k.C.....ZdSN....*.K....<Z ....G.(...`f31.1u..U.y ...`... ..>.b...XG....`Wl.X..ryI..... ...ml.2.....x:..7.D....da. f)...&..n\.B.....L..>e..... .....b L%....%...Q.c... .....e.V_.M.$pV.q..Q..n.@. y..*u.z5 l..e2[V.	success or wait	9	403091	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsaC339.tmp\2zz1gp0k.dll	unknown	5120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 10 e8 92 3b 54 89 fc 68 54 89 fc 68 54 89 fc 68 40 e2 fd 69 47 89 fc 68 54 89 fd 68 7b 89 fc 68 f1 e0 f8 69 55 89 fc 68 f1 e0 fc 69 55 89 fc 68 f1 e0 03 68 55 89 fc 68 f1 e0 fe 69 55 89 fc 68 52 69 63 68 54 89 fc 68 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 17 62 6e 60 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 10 00 02 00 00 00 10 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........;T..hT..hT..h@..iG. .hT..h{..h...iU..h...iU..h...h U..h...iU..hRichT..h.......... ......PE..L....bn`..........!	success or wait	1	403017	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\mal5.exe	unknown	512	success or wait	74	4030EA	ReadFile
C:\Users\user\Desktop\mal5.exe	unknown	4	success or wait	1	4030EA	ReadFile
C:\Users\user\Desktop\mal5.exe	unknown	4	success or wait	3	4030EA	ReadFile
C:\Users\user\AppData\Local\Temp\627zxnx9ige	unknown	12805	success or wait	1	733610AC	ReadFile
C:\Users\user\AppData\Local\Temp\x1y8d3vne767i3k	unknown	292864	success or wait	1	2B72520	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B70849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B70849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B70849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B70849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B70849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B70849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2B70849	ReadFile

Analysis Process: mal5.exe PID: 4672 Parent PID: 400

General

Start time:	12:30:20
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\mal5.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\mal5.exe'
Imagebase:	0x400000
File size:	340902 bytes
MD5 hash:	082B50AA4A4CCAEA6B415DE2E968AD47
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: 00000001.00000001.235962942.0000000000414000.00000040.00020000.sdmp, Author: Joe Security

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA7CF06	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	6DA7CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8C1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C8C1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C8C1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\45c7a76f-7fa3-431f-a653-f9a604e01987	unknown	4096	success or wait	1	6C8C1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C8C1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C8C1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C8C1B4F	ReadFile

Disassembly

Code Analysis