ID: 344977
Sample Name: AE-808_RAJEN.exe
Cookbook: default.jbs
Time: 15:17:15
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

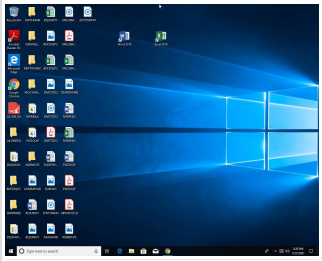
Analysis Report AE-808_RAJEN.exe

Overview

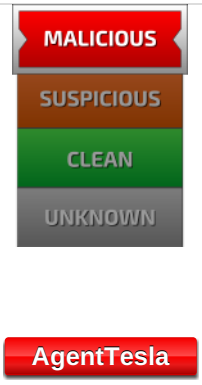
General Information

Sample Name:	AE-808_RAJEN.exe
Analysis ID:	344977
MD5:	208f2494a82c3b8.
SHA1:	98f350298f0b61c..
SHA256:	a659c50e03822c..
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection



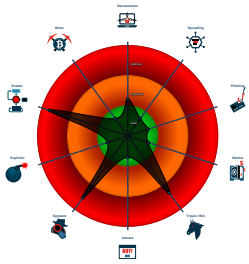
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Queries sensitive video device inform…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- AE-808_RAJEN.exe (PID: 6140 cmdline: 'C:\Users\user\Desktop\AE-808_RAJEN.exe' MD5: 208F2494A82C3B830D676C187E1F03D1)
  - AE-808_RAJEN.exe (PID: 2912 cmdline: C:\Users\user\Desktop\AE-808_RAJEN.exe MD5: 208F2494A82C3B830D676C187E1F03D1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "=0AcmYy16kpc",
  "URL: ": "https://EiR6SA0ya1Q.org",
  "To: ": "bluez@hisensetech.gq",
  "ByHost: ": "server116.web-hosting.com:587",
  "Password: ": "=0AvNB2DkamI",
  "From: ": "bluezlog@hisensetech.gq"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.654461075.0000000002B91000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.654506944.0000000002BCE000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.654789370.0000000003B99000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.654908714.0000000003C86000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.1030691966.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 6 entries				

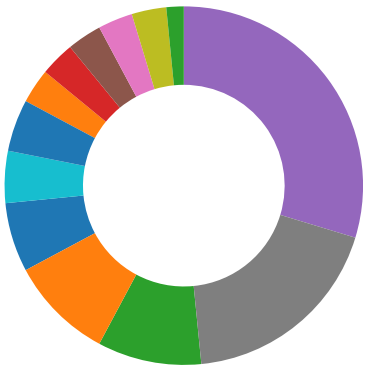
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.AE-808_RAJEN.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

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

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

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

Queries sensitive video device information (via WMI, Win32_VideoController, 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

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

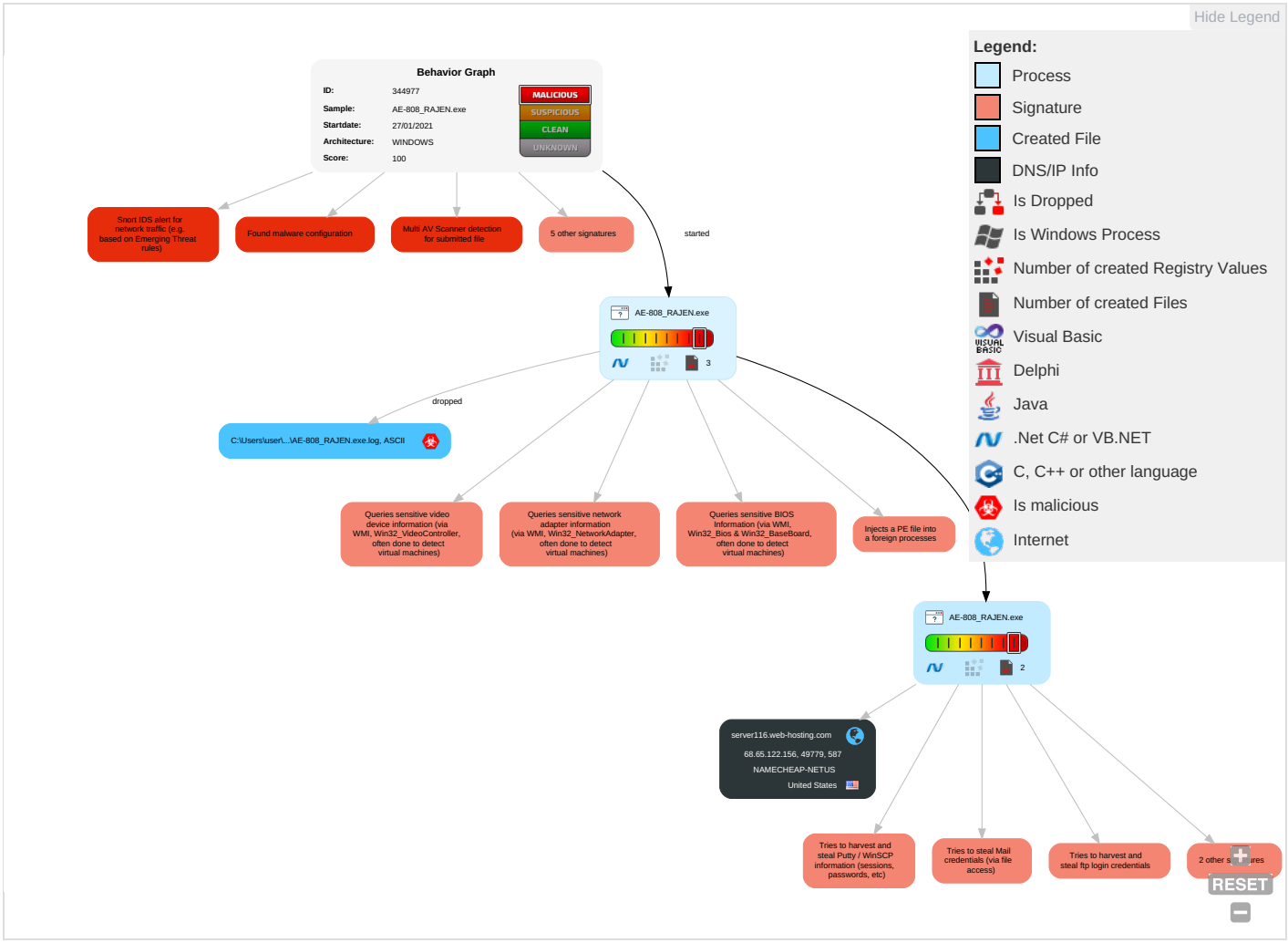
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Valid Accounts	Windows Management Instrumentation 3 1 1	Path Interception	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Stand Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Appli Layer Prot
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Application Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 2 4	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 4	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto

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
AE-808_RAJEN.exe	35%	Virustotal		Browse
AE-808_RAJEN.exe	37%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
AE-808_RAJEN.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.AE-808_RAJEN.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://EiR6SA0ya1Q.org	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://EiR6SA0ya1Q.or	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://api.lightboot.org/panel/index.php?page=Api&key=b6udeJ2WqDoyHKzzsEjfG3QajboCjeJv&host=	0%	Avira URL Cloud	safe	
http://lOlcWJ.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
server116.web-hosting.com	68.65.122.156	true	false		high

Contacted URLs

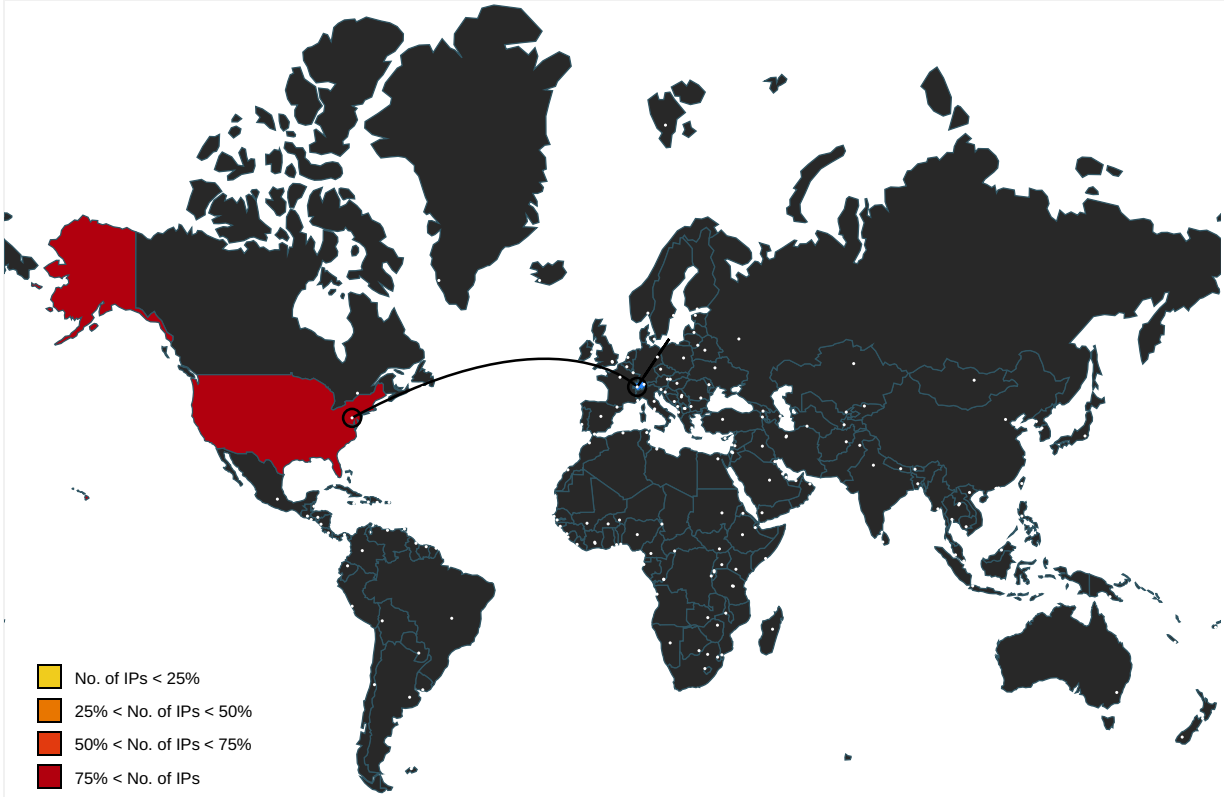
Name	Malicious	Antivirus Detection	Reputation
http://https://EiR6SA0ya1Q.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	AE-808_RAJEN.exe, 00000001.00000002.1032201040.0000000003341000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	AE-808_RAJEN.exe, 00000001.00000002.1032201040.0000000003341000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://EiR6SA0ya1Q.or	AE-808_RAJEN.exe, 00000001.00000002.1032201040.0000000003341000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://server116.web-hosting.com	AE-808_RAJEN.exe, 00000001.00000002.1032679809.00000000036A5000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	AE-808_RAJEN.exe, 00000001.00000002.1032201040.0000000003341000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.lightboot.org/panel/index.php?page=Api&key=b6udeJ2WqDoyHKzzsEjfG3QajboCjeJv&host=	AE-808_RAJEN.exe	false	• Avira URL Cloud: safe	unknown
http://https://simpletimelapse.sourceforge.io/update/changelog.txt	AE-808_RAJEN.exe	false		high
http://lOlcWJ.com	AE-808_RAJEN.exe, 00000001.00000002.1032201040.0000000003341000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://simpletimelapse.sourceforge.net/update/version.txt?Refresh=	AE-808_RAJEN.exe	false		high
http://https://ffmpeg.org	AE-808_RAJEN.exe	false		high
http://https://simpletimelapse.sourceforge.io/update/version.txt	AE-808_RAJEN.exe	false		high
http://https://www.flaticon.com/packs/free-basic-ui-elements	AE-808_RAJEN.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	AE-808_RAJEN.exe, 00000000.00000002.654461075.0000000002B91000.00000004.00000001.sdmp	false		high
http:// https://simpletimelapse.sourceforge.io/update/version.txtwhttps://simpletimelapse.sourceforge.io/upd	AE-808_RAJEN.exe	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	AE-808_RAJEN.exe, 00000000.00000002.654789370.0000000003B99000.00000004.00000001.sdmp, AE-808_RAJEN.exe, 00000001.00000002.1030691966.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
68.65.122.156	unknown	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344977
Start date:	27.01.2021
Start time:	15:17:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AE-808_RAJEN.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17

Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 65.2% • Quality standard deviation: 7.4%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 52.147.198.201, 40.88.32.150, 13.64.90.137, 51.104.139.180, 95.101.22.216, 95.101.22.224, 52.155.217.156, 20.54.26.129, 95.101.27.163, 95.101.27.142, 51.104.144.132 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, au.download.windowsupdate.com.edgesuite.net, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.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, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:18:03	API Interceptor	1107x Sleep call for process: AE-808_RAJEN.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
68.65.122.156	http://https://goldeded.website/?email=amltbXkuYnV0Y2hlckBraXdpYmFuay5jby5ueg==	Get hash	malicious	Browse	
	Adobe-SSPFShare.htm	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	RFQ Tengco_270121.doc	Get hash	malicious	Browse	• 198.54.122.60
	quote20210126.exe.exe	Get hash	malicious	Browse	• 198.54.117.215
	MV TAN BINH 135.pdf.exe	Get hash	malicious	Browse	• 198.54.116.236
	IMG_155710.doc	Get hash	malicious	Browse	• 199.192.18.134
	bXFjrxjRlb.exe	Get hash	malicious	Browse	• 198.54.117.215
	Dridex-06-bc1b.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	Dridex-06-bc1b.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	winlog(1).exe	Get hash	malicious	Browse	• 198.54.117.216
	Revise Bank Details_pdf.exe	Get hash	malicious	Browse	• 198.54.116.236
	SecuriteInfo.com.BehavesLike.Win32.Generic.tz.exe	Get hash	malicious	Browse	• 198.187.31.7
	SecuriteInfo.com.Trojan.DownLoader36.37393.29158.exe	Get hash	malicious	Browse	• 198.187.31.7
	Payment Swift Copy_USD 206,832,000.00.pdf.exe	Get hash	malicious	Browse	• 198.54.116.236
	INGNhYonmgtGZ9Updf.exe	Get hash	malicious	Browse	• 198.54.117.244
	DSksliT85D.exe	Get hash	malicious	Browse	• 199.188.200.97
	file.exe	Get hash	malicious	Browse	• 198.54.116.236
	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	• 104.219.248.112
	file.exe	Get hash	malicious	Browse	• 198.54.116.236
	RevisedPO.24488_pdf.exe	Get hash	malicious	Browse	• 198.54.117.215
	74725794.exe	Get hash	malicious	Browse	• 198.54.122.60
	SAMSUNG C&T UPCOMING PROJECTS19-027-MP-010203.exe.exe	Get hash	malicious	Browse	• 198.54.117.212

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AE-808_RAJEN.exe.log	
Process:	C:\Users\user\Desktop\AE-808_RAJEN.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1406
Entropy (8bit):	5.341099307467139
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmER:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHg
MD5:	E5FA1A53BA6D70E18192AF6AF7CFDBFA
SHA1:	1C076481F11366751B8DA795C98A54DE8D1D82D5
SHA-256:	1D7BAA6D3EB5A504FD4652BC01A0864DEE898D35D9E29D03EB4A60B0D6405D83
SHA-512:	77850814E24DB48E3DDF9DF5B6A8110EE1A823BAABA800F89CD353EAC7F72E48B13F3F4A4DC8E5F0FAA707A7F14ED90577CF1CB106A0422F0BEDD1EFD2E940E4
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AE-808_RAJEN.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.233193874678061
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	AE-808_RAJEN.exe
File size:	865792
MD5:	208f2494a82c3b830d676c187e1f03d1
SHA1:	98f350298f0b61cfd94c73bca51ef61802188527
SHA256:	a659c50e03822cd595bf5d21007b2870fda97b6d4a5d384 0d68bf8f333cc47ea
SHA512:	46ba20d289b65037851c5658d29a5325d90f9ede131075 6750428e54befe6f45c5169e31581560899bc9e1d7c90b0 66493d2d4e0d2bbaccaae56103437837d63
SSDEEP:	12288:tcd3/l3lFULj81T1No2u2k8Iqpy5/N/MZBCs0vvG7 PH71UF+Z:i9MLj8pLor2k8ISGVM2qqu
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..X.....v... .....@.. .....@.....

File Icon

Icon Hash:	f0f06094c36ee8c2

Static PE Info

General

Entrypoint:	0x4c761e
Entrypoint Section:	.text
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:	0x6010BABF [Wed Jan 27 00:58:39 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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
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 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc75cc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc8000	0xd8c4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd6000	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	
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	0xc5624	0xc5800	False	0.678047122231	data	7.26312302148	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc8000	0xd8c4	0xda00	False	0.0875501720183	data	3.73503425467	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd6000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc8130	0xd228	data		
RT_GROUP_ICON	0xd5358	0x14	data		
RT_VERSION	0xd536c	0x36c	data		
RT_MANIFEST	0xd56d8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

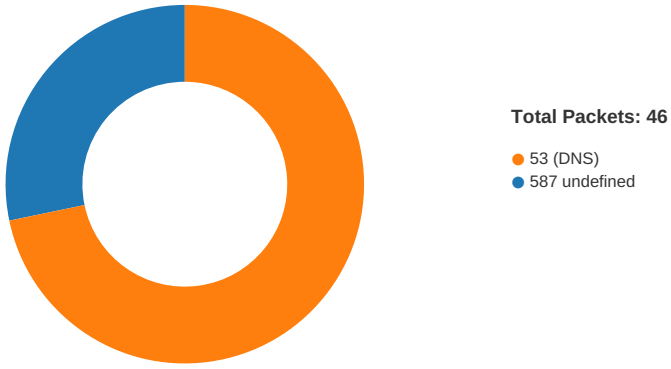
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	XmlToFieldTypeMap.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	BowenTheatre.Bookings
ProductVersion	1.0.0.0
FileDescription	BowenTheatre.Bookings
OriginalFilename	XmlToFieldTypeMap.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/21-15:19:45.470151	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49779	587	192.168.2.4	68.65.122.156

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:19:43.646884918 CET	49779	587	192.168.2.4	68.65.122.156
Jan 27, 2021 15:19:43.843363047 CET	587	49779	68.65.122.156	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:19:43.843628883 CET	49779	587	192.168.2.4	68.65.122.156
Jan 27, 2021 15:19:44.222095013 CET	587	49779	68.65.122.156	192.168.2.4
Jan 27, 2021 15:19:44.223944902 CET	49779	587	192.168.2.4	68.65.122.156
Jan 27, 2021 15:19:44.420578957 CET	587	49779	68.65.122.156	192.168.2.4
Jan 27, 2021 15:19:44.422414064 CET	49779	587	192.168.2.4	68.65.122.156
Jan 27, 2021 15:19:44.621649027 CET	587	49779	68.65.122.156	192.168.2.4
Jan 27, 2021 15:19:44.623871088 CET	49779	587	192.168.2.4	68.65.122.156
Jan 27, 2021 15:19:44.859030962 CET	587	49779	68.65.122.156	192.168.2.4
Jan 27, 2021 15:19:44.860151052 CET	49779	587	192.168.2.4	68.65.122.156
Jan 27, 2021 15:19:45.056664944 CET	587	49779	68.65.122.156	192.168.2.4
Jan 27, 2021 15:19:45.057215929 CET	49779	587	192.168.2.4	68.65.122.156
Jan 27, 2021 15:19:45.269867897 CET	587	49779	68.65.122.156	192.168.2.4
Jan 27, 2021 15:19:45.270452023 CET	49779	587	192.168.2.4	68.65.122.156
Jan 27, 2021 15:19:45.468225002 CET	587	49779	68.65.122.156	192.168.2.4
Jan 27, 2021 15:19:45.468254089 CET	587	49779	68.65.122.156	192.168.2.4
Jan 27, 2021 15:19:45.470150948 CET	49779	587	192.168.2.4	68.65.122.156
Jan 27, 2021 15:19:45.470417976 CET	49779	587	192.168.2.4	68.65.122.156
Jan 27, 2021 15:19:45.471302986 CET	49779	587	192.168.2.4	68.65.122.156
Jan 27, 2021 15:19:45.471447945 CET	49779	587	192.168.2.4	68.65.122.156
Jan 27, 2021 15:19:45.668231010 CET	587	49779	68.65.122.156	192.168.2.4
Jan 27, 2021 15:19:45.669059038 CET	587	49779	68.65.122.156	192.168.2.4
Jan 27, 2021 15:19:45.679378986 CET	587	49779	68.65.122.156	192.168.2.4
Jan 27, 2021 15:19:45.726330042 CET	49779	587	192.168.2.4	68.65.122.156

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:17:57.593713045 CET	63153	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:17:57.641669035 CET	53	63153	8.8.8.8	192.168.2.4
Jan 27, 2021 15:17:58.795239925 CET	52991	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:17:58.843216896 CET	53	52991	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:02.821556091 CET	53700	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:02.870661974 CET	53	53700	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:03.755052090 CET	51726	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:03.811577082 CET	53	51726	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:05.161515951 CET	56794	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:05.209764004 CET	53	56794	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:06.631035089 CET	56534	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:06.678890944 CET	53	56534	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:07.812458992 CET	56627	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:07.863410950 CET	53	56627	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:08.591224909 CET	56621	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:08.643161058 CET	53	56621	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:09.889314890 CET	63116	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:09.937233925 CET	53	63116	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:11.132914066 CET	64078	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:11.194746971 CET	53	64078	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:13.166769981 CET	64801	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:13.215075970 CET	53	64801	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:13.974270105 CET	61721	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:14.024561882 CET	53	61721	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:15.163275957 CET	51255	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:15.224195004 CET	53	51255	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:21.854039907 CET	61522	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:21.904855013 CET	53	61522	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:26.373717070 CET	52337	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:26.431524992 CET	53	52337	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:42.282075882 CET	55046	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:42.330965042 CET	53	55046	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:42.974797010 CET	49612	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:43.031330109 CET	53	49612	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:43.608247995 CET	49285	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:43.657280922 CET	53	49285	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:43.794528008 CET	50601	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:18:43.845555067 CET	53	50601	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:44.122066021 CET	60875	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:44.175988913 CET	53	60875	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:44.639494896 CET	56448	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:44.689656973 CET	53	56448	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:45.217423916 CET	59172	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:45.270375013 CET	53	59172	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:45.823774099 CET	62420	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:45.882536888 CET	53	62420	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:46.688292980 CET	60579	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:46.747139931 CET	53	60579	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:47.333359957 CET	50183	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:47.391213894 CET	53	50183	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:47.769828081 CET	61531	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:47.820646048 CET	53	61531	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:48.325128078 CET	49228	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:48.376374960 CET	53	49228	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:59.790587902 CET	59794	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:59.838519096 CET	53	59794	8.8.8.8	192.168.2.4
Jan 27, 2021 15:18:59.903474092 CET	55916	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:18:59.953564882 CET	53	55916	8.8.8.8	192.168.2.4
Jan 27, 2021 15:19:02.797210932 CET	52752	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:19:02.858230114 CET	53	52752	8.8.8.8	192.168.2.4
Jan 27, 2021 15:19:33.748116016 CET	60542	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:19:33.798858881 CET	53	60542	8.8.8.8	192.168.2.4
Jan 27, 2021 15:19:35.795480013 CET	60689	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:19:35.856194019 CET	53	60689	8.8.8.8	192.168.2.4
Jan 27, 2021 15:19:43.481662989 CET	64206	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:19:43.538068056 CET	53	64206	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 15:19:43.481662989 CET	192.168.2.4	8.8.8.8	0x4659	Standard query (0)	server116.web-hosting.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:19:43.538068056 CET	8.8.8.8	192.168.2.4	0x4659	No error (0)	server116.web-hosting.com		68.65.122.156	A (IP address)	IN (0x0001)

SMTP Packets

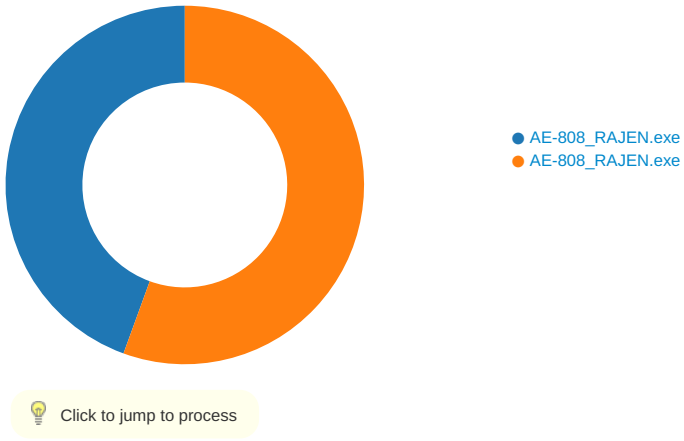
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 15:19:44.222095013 CET	587	49779	68.65.122.156	192.168.2.4	220-server116.web-hosting.com ESMTP Exim 4.93 #2 Wed, 27 Jan 2021 09:19:44 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 27, 2021 15:19:44.223944902 CET	49779	587	192.168.2.4	68.65.122.156	EHLO 571345
Jan 27, 2021 15:19:44.420578957 CET	587	49779	68.65.122.156	192.168.2.4	250-server116.web-hosting.com Hello 571345 [84.17.52.74] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jan 27, 2021 15:19:44.422414064 CET	49779	587	192.168.2.4	68.65.122.156	AUTH login Ymx1ZXpsb2dAaGlzZW5zZXRlY2guZ3E=
Jan 27, 2021 15:19:44.621649027 CET	587	49779	68.65.122.156	192.168.2.4	334 UGFzc3dvcmQ6
Jan 27, 2021 15:19:44.859030962 CET	587	49779	68.65.122.156	192.168.2.4	235 Authentication succeeded
Jan 27, 2021 15:19:44.860151052 CET	49779	587	192.168.2.4	68.65.122.156	MAIL FROM:<bluezlog@hisensetech.gq>
Jan 27, 2021 15:19:45.056664944 CET	587	49779	68.65.122.156	192.168.2.4	250 OK
Jan 27, 2021 15:19:45.057215929 CET	49779	587	192.168.2.4	68.65.122.156	RCPT TO:<bluez@hisensetech.gq>
Jan 27, 2021 15:19:45.269867897 CET	587	49779	68.65.122.156	192.168.2.4	250 Accepted
Jan 27, 2021 15:19:45.270452023 CET	49779	587	192.168.2.4	68.65.122.156	DATA
Jan 27, 2021 15:19:45.468254089 CET	587	49779	68.65.122.156	192.168.2.4	354 Enter message, ending with "." on a line by itself

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 15:19:45.471447945 CET	49779	587	192.168.2.4	68.65.122.156	.
Jan 27, 2021 15:19:45.679378986 CET	587	49779	68.65.122.156	192.168.2.4	250 OK id=1l4lfd-003v8v-CQ

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: AE-808_RAJEN.exe PID: 6140 Parent PID: 4260

General

Start time:	15:18:01
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\AE-808_RAJEN.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\AE-808_RAJEN.exe'
Imagebase:	0x670000
File size:	865792 bytes
MD5 hash:	208F2494A82C3B830D676C187E1F03D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.654461075.0000000002B91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.654506944.0000000002BCE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.654789370.0000000003B99000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.654908714.0000000003C86000.00000004.00000001.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	6D3DCF06	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	6D3DCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AE-808_RAJEN.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6EC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AE-808_RAJEN.exe.log	unknown	1406	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D6EC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile

Analysis Process: AE-808_RAJEN.exe PID: 2912 Parent PID: 6140

General

Start time:	15:18:04
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\AE-808_RAJEN.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\AE-808_RAJEN.exe
Imagebase:	0xea0000
File size:	865792 bytes
MD5 hash:	208F2494A82C3B830D676C187E1F03D1
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: 00000001.00000002.1030691966.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.1032201040.0000000003341000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.1032201040.0000000003341000.00000004.00000001.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	6D3DCF06	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	6D3DCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6C221B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\7769e121-3c02-4a2a-a2a1-14d54a0e6d3f	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6C221B4F	ReadFile

Disassembly

Code Analysis