ID: 321141
Sample Name: .exe
Cookbook: default.jbs
Time: 12:35:22
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

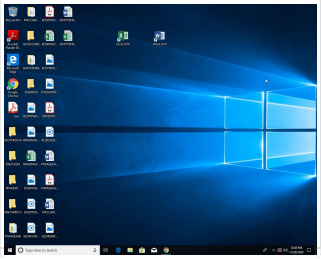
Analysis Report .exe

Overview

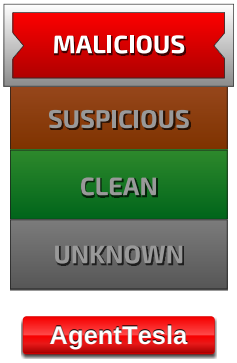
General Information

Sample Name:	.exe
Analysis ID:	321141
MD5:	4c0960a2215352..
SHA1:	8596c7561f3668d.
SHA256:	c9442156b26b8fe.
Tags:	exe

Most interesting Screenshot:



Detection

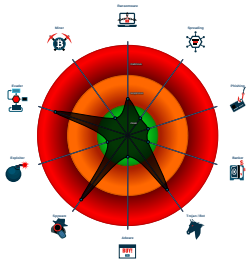


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Found malware configuration
- Icon mismatch, binary includes an ic…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Sigma detected: Suspicious Double …
- Yara detected AgentTesla
- Yara detected AntiVM_3
- Contains functionality to register a lo…
- Installs a global keyboard hook

Classification



Startup

- **System is w10x64**
- .exe (PID: 6444 cmdline: 'C:\Users\user\Desktop\ .exe' MD5: 4C0960A22153523B2626BFF364CC7073)
  - schtasks.exe (PID: 6604 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\apQsEpT' /XML 'C:\Users\user\AppData\Local\Temp\tmp88EB.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6612 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - .exe (PID: 6752 cmdline: {path} MD5: 4C0960A22153523B2626BFF364CC7073)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "LG3xhtQljnZve",
  "URL: ": "http://dIhLHGXisr.net",
  "To: ": "supervisor@persec.gr",
  "ByHost: ": "mail.persec.gr:587",
  "Password: ": "g71iC6Xh1Q24qt",
  "From: ": "supervisor@persec.gr"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
.exe	MAL_RANSOM_COVID19_Apr20_1	Detects ransomware distributed in COVID-19 theme	Florian Roth	• 0x74117:$op2: 60 2E 2E 2E AF 34 34 34 B8 34 34 34 B8 34 34 34 • 0x73a9f:$op3: 1F 07 1A 37 85 05 05 36 83 05 05 36 83 05 05 34

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\apQsEpT.exe	MAL_RANSOM_COVID19_Apr20_1	Detects ransomware distributed in COVID-19 theme	Florian Roth	• 0x74117:$op2: 60 2E 2E 2E AF 34 34 34 B8 34 34 34 B8 34 34 34 • 0x73a9f:$op3: 1F 07 1A 37 85 05 05 36 83 05 05 36 83 05 05 34

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.475265979.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.228870931.00000000038F5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.227599432.000000000289E000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.478164785.000000000293100.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.478164785.000000000293100.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2. .exe.510000.1.unpack	MAL_RANSOM_COVID19_Apr20_1	Detects ransomware distributed in COVID-19 theme	Florian Roth	• 0x74117:$op2: 60 2E 2E 2E AF 34 34 34 B8 34 34 34 B8 34 34 34 • 0x73a9f:$op3: 1F 07 1A 37 85 05 05 36 83 05 05 36 83 05 05 34
4.0. .exe.510000.0.unpack	MAL_RANSOM_COVID19_Apr20_1	Detects ransomware distributed in COVID-19 theme	Florian Roth	• 0x74117:$op2: 60 2E 2E 2E AF 34 34 34 B8 34 34 34 B8 34 34 34 • 0x73a9f:$op3: 1F 07 1A 37 85 05 05 36 83 05 05 36 83 05 05 34
0.0. .exe.320000.0.unpack	MAL_RANSOM_COVID19_Apr20_1	Detects ransomware distributed in COVID-19 theme	Florian Roth	• 0x74117:$op2: 60 2E 2E 2E AF 34 34 34 B8 34 34 34 B8 34 34 34 • 0x73a9f:$op3: 1F 07 1A 37 85 05 05 36 83 05 05 36 83 05 05 34
4.2. .exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2. .exe.320000.0.unpack	MAL_RANSOM_COVID19_Apr20_1	Detects ransomware distributed in COVID-19 theme	Florian Roth	• 0x74117:$op2: 60 2E 2E 2E AF 34 34 34 B8 34 34 34 B8 34 34 34 • 0x73a9f:$op3: 1F 07 1A 37 85 05 05 36 83 05 05 36 83 05 05 34

Sigma Overview

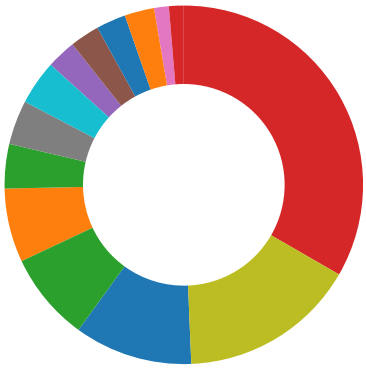
System Summary:

Sigma detected: Scheduled temp file as task from temp location

Sigma detected: Suspicious Double Extension

Signature Overview

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



Click to jump to signature section

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Contains functionality to register a low level keyboard hook
- Installs a global keyboard hook

System Summary:

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

- Icon mismatch, binary includes an icon from a different legit application in order to fool users

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

Stealing of Sensitive Information:

- Yara detected AgentTesla
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
- Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

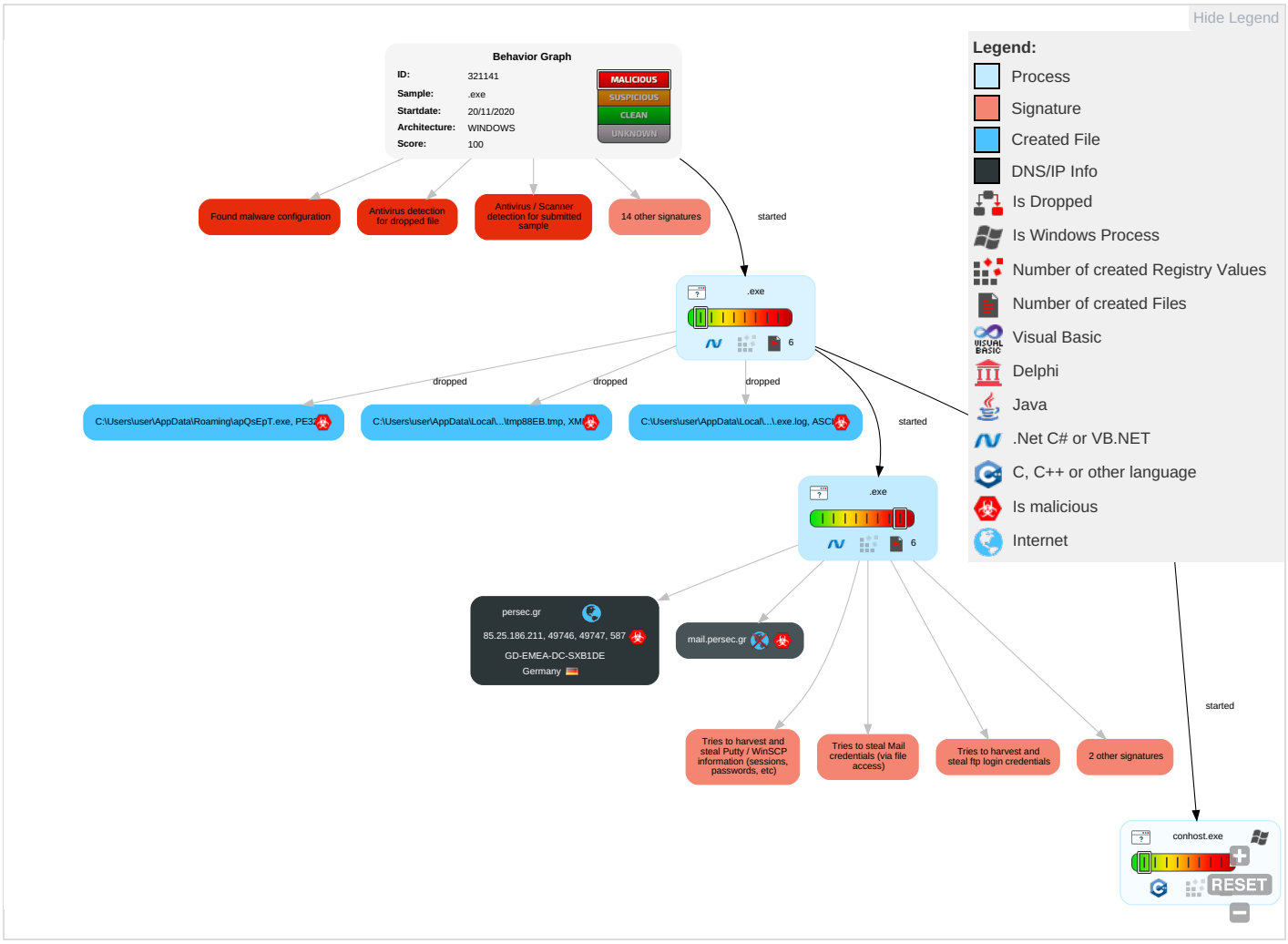
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

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

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
.exe	56%	Virustotal		Browse
.exe	42%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
.exe	100%	Avira	TR/Kryptik.uduze	
.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\apQsEpT.exe	100%	Avira	TR/Kryptik.uduze	
C:\Users\user\AppData\Roaming\apQsEpT.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\apQsEpT.exe	42%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2. .exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
persec.gr	0%	Virustotal		Browse
mail.persec.gr	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	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://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://GMgRDJ.com	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://mail.persec.gr	0%	Avira URL Cloud	safe	
http://dIhLHGXisr.net	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://dIhLHGXisr.ne	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://persec.gr	0%	Avira URL Cloud	safe	
http://dIhLHGXisr.net1-5-21-3853321935-2125563209-4053062332-1002_Classes	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://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
persec.gr	85.25.186.211	true	true	• 0%, Virustotal, Browse	unknown
mail.persec.gr	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

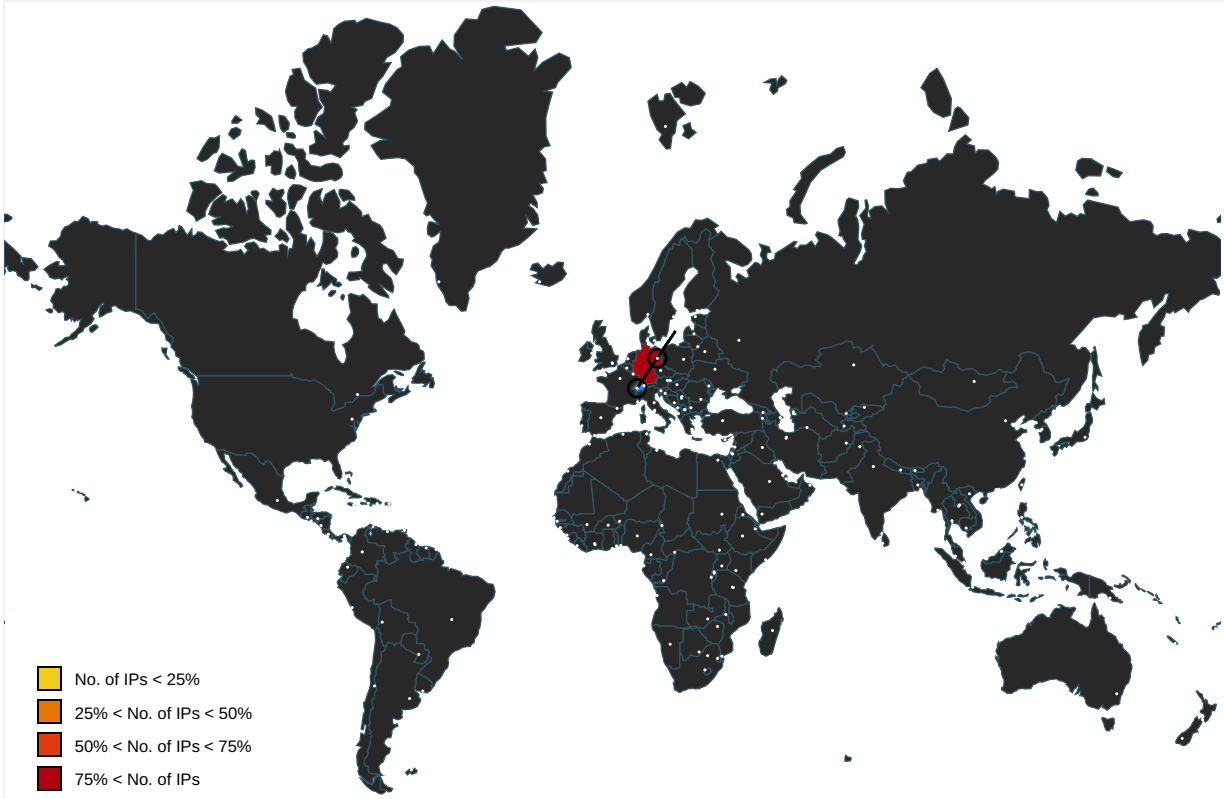
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	.exe, 00000004.0000000 2.478164785.0000000002931000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false		high
http://www.fontbureau.com	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	.exe, 00000004.0000000 2.478164785.0000000002931000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	.exe, 00000004.0000000 2.480867921.0000000002CE3000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/ 9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	.exe, 00000004.0000000 2.478164785.0000000002931000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://GMgRDJ.com	.exe, 00000004.0000000 2.478164785.0000000002931000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.persec.gr	.exe, 00000004.0000000 2.480546013.0000000002C91000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false		high
http://dIhLHGXisr.net	.exe, 00000004.0000000 2.478164785.0000000002931000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://dIhLHGXisr.ne	.exe, 00000004.0000000 2.478164785.0000000002931000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	.exe, 00000004.0000000 2.478164785.0000000002931000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/	.exe, 00000000.0000000 2.228870931.00000000038F5000.0 0000004.00000001.sdmp, .exe, 00000004.00000002.475265979.00000 00000402000.00000040.00000001. sdmp	false		high
http://www.jiyu-kobo.co.jp/	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false		high
http://persec.gr	.exe, 00000004.0000000 2.480546013.0000000002C91000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://dIhLHGXisr.net1-5-21-3853321935-2125563209-4053062332-1002_Classes	.exe, 00000004.0000000 3.432962878.0000000000994000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fonts.com	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	.exe, 00000000.0000000 2.227280957.0000000002851000.0 0000004.00000001.sdmp	false		high
http://www.sakkal.com	.exe, 00000000.0000000 2.233363477.000000000BC32000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	.exe, 00000004.0000000 2.478164785.0000000002931000.0 0000004.00000001.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	.exe, 00000000.0000000 2.228870931.00000000038F5000.0 0000004.00000001.sdmp, .exe, 00000004.00000002.475265979.00000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.25.186.211	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321141
Start date:	20.11.2020
Start time:	12:35:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 47s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	.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:	23
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@6/4@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.6% (good quality ratio 0.6%) • Quality average: 60.4% • Quality standard deviation: 23.4%
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:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 52.147.198.201, 104.43.193.48, 104.75.88.60, 51.104.139.180, 20.54.26.129, 205.185.216.42, 205.185.216.10, 40.67.251.132, 95.101.22.134, 95.101.22.125, 204.79.197.200, 13.107.21.200 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, par02p.wns.notify.windows.com.akadns.net, db5p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, www-bing-com.dual-a-0001.a-msedge.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, a-0001.a-afdentry.net.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 NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:36:17	API Interceptor	794x Sleep call for process: .exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GD-EMEA-DC-SXB1DE	malware.html	Get hash	malicious	Browse	• 188.93.15.103
	http://your-prize-ready-lkz.live/?u=1nup806&o=0wywy2l&t=k2Dr_USAtest_PC	Get hash	malicious	Browse	• 188.138.11 1.121
	8miw6WNHCt.exe	Get hash	malicious	Browse	• 217.172.179.54
	gGTQ8uae5s.exe	Get hash	malicious	Browse	• 217.172.179.54
	ENJ5AB3B0x.exe	Get hash	malicious	Browse	• 217.172.179.54
	0P0cZbXEbK.exe	Get hash	malicious	Browse	• 217.172.179.54
	Tk8cA6bHRS.exe	Get hash	malicious	Browse	• 217.172.179.54
	fTAYoI22iY.exe	Get hash	malicious	Browse	• 217.172.179.54
	start.exe	Get hash	malicious	Browse	• 85.25.213.211
	uvjAwriS1c.exe	Get hash	malicious	Browse	• 217.172.179.54
	vAstEpls9R.exe	Get hash	malicious	Browse	• 217.172.179.54
	hmB9yvFv40.exe	Get hash	malicious	Browse	• 217.172.179.54
	ZYhucZndrm.exe	Get hash	malicious	Browse	• 217.172.179.54
	4WD28ZoLXN.exe	Get hash	malicious	Browse	• 217.172.179.54
	VLmFsICPqL.exe	Get hash	malicious	Browse	• 217.172.179.54
	Zped7c3dam.exe	Get hash	malicious	Browse	• 217.172.179.54
	idWMSrWvoE.exe	Get hash	malicious	Browse	• 87.230.25.43
	cK2ClsvtJE.exe	Get hash	malicious	Browse	• 87.230.25.43
	AXZFXiJCj3.exe	Get hash	malicious	Browse	• 87.230.25.43
	lHuFdWpoMA.exe	Get hash	malicious	Browse	• 87.230.25.43

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\ .exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ .exe.log	
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4VE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz5
MD5:	6C42AAF2F2FABAD2BAB70543AE48CEDB
SHA1:	8552031F83C078FE1C035191A32BA43261A63DA9
SHA-256:	51D07DD061EA9665DA070B95A4AC2AC17E20524E30BF6A0DA8381C2AF29CA967
SHA-512:	014E89857B811765EA7AA0B030AB04A2DA1957571608C4512EC7662F6A4DCE8B0409626624DABC96CBFF079E7F0F4A916E6F49C789E00B6E46AD37C36C806DC
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp88EB.tmp	
Process:	C:\Users\user\Desktop\ .exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1640
Entropy (8bit):	5.184896527826423
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBxBtn:cbh47TlNQ//rydbz9I3YODOLNdq3n
MD5:	6EAB4206B94D6528E932EC3C4A938DCC
SHA1:	20BA86B7BC00D2BDD0FEDAC3C5CA48D7B8852CB0
SHA-256:	5A05D19A5B06DD9FCFBD0A0A4229A8472721905D99841944B0792E0AFC2A2D47
SHA-512:	644E57F4BB285CECEE145FD85513016EE55CE10AA0AD7A3E9EFF25F3A6C833D6832A3AAC4B3208199B1F64D48D47B3B638A15906EE5EA548FC667D36B3B142E7
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\51qhj2rq.aji\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\ .exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Roaming\apQsEpT.exe	
Process:	C:\Users\user\Desktop\ .exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	561664
Entropy (8bit):	7.555510842518211
Encrypted:	false

C:\Users\user\AppData\Roaming\apQsEpT.exe	
SSDEEP:	12288:Y19HzS46VFkxNjZ53CBc8860il614WNHJ6vPdJxxcaOq1MUCTdAA:Y19OzVFkxNjLyJ8ytHAvPdWA
MD5:	4C0960A22153523B2626BFF364CC7073
SHA1:	8596C7561F3668D544EE5CF24AC19C1C9DB6C616
SHA-256:	C9442156B26B8FE68A84028F85861191BFF85680B1460D26B9491CBC3F3AC230
SHA-512:	7CB0051E450BF16547B891309C8E51E51B41F3F8F95EE2F15FC5DAC0B3DA6683B74EC65942CEA03CD03F60BEDFFA2760D5B7754EB73537CFCDDAABF1B1BB68ED
Malicious:	**true**
Yara Hits:	• Rule: MAL_RANSOM_COVID19_Apr20_1, Description: Detects ransomware distributed in COVID-19 theme, Source: C:\Users\user\AppData\Roaming\apQsEpT.exe, Author: Florian Roth
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 42%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....N.... ... .@.. ....@.....S.... ....H.....text...T.... ....`.rsrc..... .....@..@.reloc..... .....@..B.....0.....H.....B.....h.....).....Z.....H...@.#...t.....C(...HB.p..=.\| ...98...:%:2xRw...wG.(F"....M 9b.].\4`7...q...V..K.....m..i.\...B&....z...l...k.....)_...q..l7.z..Il..G....el..$..Y....Zb['A?....y.M..9.y.|.`F/..N..T2....E...V.o..'...e.0..7...@..q1.~d.s[....b.T7|..1.....L.2I...$.rnB..9.+j..(..(. .....Sgz..hd....#I...=..46..J._D.t.1.V.d....{?..1.`.A...:...L.....*!M.}p...<2..<...n.M..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.555510842518211
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	.exe
File size:	561664
MD5:	4c0960a22153523b2626bff364cc7073
SHA1:	8596c7561f3668d544ee5cf24ac19c1c9db6c616
SHA256:	c9442156b26b8fe68a84028f85861191bff85680b1460d26b9491cbc3f3ac230
SHA512:	7cb0051e450bf16547b891309c8e51e51b41f3f8f95ee2f15fc5dac0b3da6683b74ec65942cea03cd03f60bedffa2760d5b7754eb73537cfcddaabf1b1bb68ed
SSDEEP:	12288:Y19HzS46VFkxNjZ53CBc8860il614WNHJ6vPdJxxcaOq1MUCTdAA:Y19OzVFkxNjLyJ8ytHAvPdWA
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....N.... ... .@.. .....@.....

File Icon

Icon Hash:	6eeccccd6d2f2f2

Static PE Info

General

Entrypoint:	0x471e4e
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:	0x5FB72EF8 [Fri Nov 20 02:50:32 2020 UTC]

General

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

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
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	0x71df8	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x72000	0x18d18	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8c000	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

Name	Virtual Address	Virtual Size	Is in Section
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	0x6fe54	0x70000	False	0.898808070592	data	7.8624495092	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x72000	0x18d18	0x18e00	False	0.14752473304	data	4.30896630278	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8c000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x72220	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x747c8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x75870	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x75cd8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x79f00	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0x8a728	0x4c	data		
RT_GROUP_ICON	0x8a774	0x14	data		
RT_VERSION	0x8a788	0x39e	data		
RT_MANIFEST	0x8ab28	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

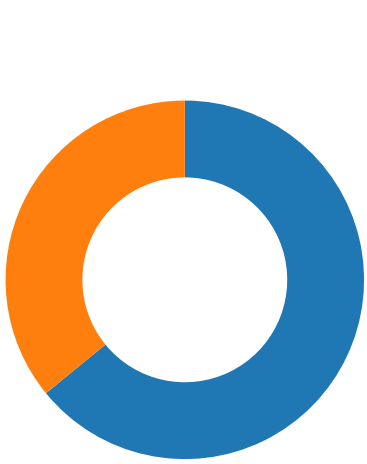
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Les loups-garous de Thiercelieux 1998
Assembly Version	27.0.0.0
InternalName	.exe
FileVersion	11.0.0.0
CompanyName	Les loups-garous de Thiercelieux
LegalTrademarks	
Comments	Jeu de la barbichette
ProductName	Ptanque
ProductVersion	11.0.0.0
FileDescription	Ptanque
OriginalFilename	.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:38:00.977946997 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:00.997334003 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:00.997428894 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:01.926336050 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:01.926994085 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:01.946588993 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:01.946995974 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:01.968089104 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.023704052 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.045360088 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.072175980 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.072227001 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.072264910 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.072293043 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.072474957 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.073900938 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.117549896 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.123652935 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.143440962 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.195578098 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.466299057 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.486628056 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.488738060 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.509500980 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.510548115 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.553603888 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.554804087 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.574997902 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.575711012 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.618599892 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.619195938 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.639064074 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.642260075 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.642452955 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.643198967 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.643356085 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.643507004 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.643609047 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.643724918 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:02.662549973 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.662569046 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.663698912 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.663716078 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.663774014 CET	587	49746	85.25.186.211	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:38:02.663813114 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.663898945 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.671686888 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:02.725683928 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:03.741187096 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:03.761964083 CET	587	49746	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:03.762187004 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:03.903204918 CET	49746	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:03.904203892 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:03.924031973 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:03.924173117 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:04.842757940 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:04.845351934 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:04.923455954 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:04.925406933 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:04.947405100 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:04.949417114 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:04.973270893 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:04.973308086 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:04.973361969 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:04.973392010 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:04.973479986 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:04.973524094 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:04.974612951 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:04.977596045 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:04.997344017 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:05.002207041 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:05.021641016 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:05.025597095 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:05.045763969 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:05.048933983 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:05.077080011 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:05.077486038 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:05.097053051 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:05.097573996 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:05.119723082 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:05.121519089 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:05.141120911 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:05.145776033 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:05.145817995 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:05.145965099 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:05.146074057 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:05.146205902 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:05.146271944 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:05.146338940 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:05.146420956 CET	49747	587	192.168.2.3	85.25.186.211
Nov 20, 2020 12:38:05.166944027 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:05.167006969 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:05.167032957 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:05.167191029 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:05.167347908 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:05.167506933 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:05.167700052 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:05.168315887 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:05.196713924 CET	587	49747	85.25.186.211	192.168.2.3
Nov 20, 2020 12:38:05.242696047 CET	49747	587	192.168.2.3	85.25.186.211

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:36:08.970140934 CET	65110	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:09.005853891 CET	53	65110	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:13.681493998 CET	58361	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:14.671353102 CET	58361	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:36:14.717644930 CET	53	58361	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:15.517726898 CET	63492	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:15.544877052 CET	53	63492	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:17.256653070 CET	60831	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:17.292351961 CET	53	60831	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:17.983359098 CET	60100	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:18.019092083 CET	53	60100	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:18.801959991 CET	53195	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:18.829180956 CET	53	53195	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:21.611474991 CET	50141	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:21.638576984 CET	53	50141	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:23.167923927 CET	53023	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:23.205724955 CET	53	53023	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:24.022481918 CET	49563	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:24.049583912 CET	53	49563	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:24.834919930 CET	51352	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:24.862096071 CET	53	51352	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:25.474847078 CET	59349	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:25.502132893 CET	53	59349	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:26.763196945 CET	57084	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:26.798861027 CET	53	57084	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:27.468164921 CET	58823	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:27.495323896 CET	53	58823	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:29.045761108 CET	57568	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:29.072999954 CET	53	57568	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:31.155839920 CET	50540	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:31.193155050 CET	53	50540	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:39.031672955 CET	54366	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:39.069062948 CET	53	54366	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:40.108289003 CET	53034	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:40.135490894 CET	53	53034	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:55.898308039 CET	57762	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:55.925498962 CET	53	57762	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:58.443252087 CET	55435	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:58.470415115 CET	53	55435	8.8.8.8	192.168.2.3
Nov 20, 2020 12:36:59.801129103 CET	50713	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:36:59.838229895 CET	53	50713	8.8.8.8	192.168.2.3
Nov 20, 2020 12:37:01.485153913 CET	56132	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:37:01.512511015 CET	53	56132	8.8.8.8	192.168.2.3
Nov 20, 2020 12:37:08.559787989 CET	58987	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:37:08.595463991 CET	53	58987	8.8.8.8	192.168.2.3
Nov 20, 2020 12:37:09.859808922 CET	56579	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:37:09.897067070 CET	53	56579	8.8.8.8	192.168.2.3
Nov 20, 2020 12:37:49.360775948 CET	60633	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:37:49.387875080 CET	53	60633	8.8.8.8	192.168.2.3
Nov 20, 2020 12:37:49.887111902 CET	61292	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:37:49.914369106 CET	53	61292	8.8.8.8	192.168.2.3
Nov 20, 2020 12:38:00.741539001 CET	63619	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:38:00.805789948 CET	53	63619	8.8.8.8	192.168.2.3
Nov 20, 2020 12:38:00.840876102 CET	64938	53	192.168.2.3	8.8.8.8
Nov 20, 2020 12:38:00.891570091 CET	53	64938	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 12:38:00.741539001 CET	192.168.2.3	8.8.8.8	0xaf0f	Standard query (0)	mail.persec.gr	A (IP address)	IN (0x0001)
Nov 20, 2020 12:38:00.840876102 CET	192.168.2.3	8.8.8.8	0xeec7	Standard query (0)	mail.persec.gr	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 12:38:00.805789948 CET	8.8.8.8	192.168.2.3	0xaf0f	No error (0)	mail.persec.gr	persec.gr		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:38:00.805789948 CET	8.8.8.8	192.168.2.3	0xaf0f	No error (0)	persec.gr		85.25.186.211	A (IP address)	IN (0x0001)
Nov 20, 2020 12:38:00.891570091 CET	8.8.8.8	192.168.2.3	0xeec7	No error (0)	mail.persec.gr	persec.gr		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:38:00.891570091 CET	8.8.8.8	192.168.2.3	0xeec7	No error (0)	persec.gr		85.25.186.211	A (IP address)	IN (0x0001)

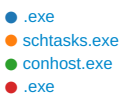
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 20, 2020 12:38:01.926336050 CET	587	49746	85.25.186.211	192.168.2.3	220-qla.angellight.com ESMTP Exim 4.93 #2 Fri, 20 Nov 2020 13:38:01 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 20, 2020 12:38:01.926994085 CET	49746	587	192.168.2.3	85.25.186.211	EHLO 760639
Nov 20, 2020 12:38:01.946588993 CET	587	49746	85.25.186.211	192.168.2.3	250-qla.angellight.com Hello 760639 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 20, 2020 12:38:01.946995974 CET	49746	587	192.168.2.3	85.25.186.211	STARTTLS
Nov 20, 2020 12:38:01.968089104 CET	587	49746	85.25.186.211	192.168.2.3	220 TLS go ahead
Nov 20, 2020 12:38:04.842757940 CET	587	49747	85.25.186.211	192.168.2.3	220-qla.angellight.com ESMTP Exim 4.93 #2 Fri, 20 Nov 2020 13:38:04 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 20, 2020 12:38:04.845351934 CET	49747	587	192.168.2.3	85.25.186.211	EHLO 760639
Nov 20, 2020 12:38:04.923455954 CET	587	49747	85.25.186.211	192.168.2.3	250-qla.angellight.com Hello 760639 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 20, 2020 12:38:04.925406933 CET	49747	587	192.168.2.3	85.25.186.211	STARTTLS
Nov 20, 2020 12:38:04.947405100 CET	587	49747	85.25.186.211	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: .exe PID: 6444 Parent PID: 5652

General

Start time:	12:36:12
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\ .exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ .exe'
Imagebase:	0x320000
File size:	561664 bytes
MD5 hash:	4C0960A22153523B2626BFF364CC7073
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.228870931.00000000038F5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.227599432.000000000289E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.229056659.0000000003AF5000.00000004.00000001.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	6E12CF06	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	6E12CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\apQsEpT.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF71E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp88EB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF77038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ .exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E43C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp88EB.tmp	success or wait	1	6CF76A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\apQsEpT.exe	unknown	561664	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 f8 2e b7 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 00 07 00 00 90 01 00 00 00 00 00 4e 1e 07 00 00 20 00 00 00 20 07 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 e0 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......_.......... ....N.... ... .@.. ....@................	success or wait	1	6CF71B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp88EB.tmp	unknown	1640	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6CF71B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ .exe.log	unknown	1301	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 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 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 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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_v4.0.3	success or wait	1	6E43C907	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	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E105705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E10CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF71B4F	ReadFile
C:\Users\user\Desktop\ .exe	unknown	561664	success or wait	1	6CF71B4F	ReadFile

Analysis Process: schtasks.exe PID: 6604 Parent PID: 6444

General

Start time:	12:36:18
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\apQsEpT' /XML 'C:\Users\ user\AppData\Local\Temp\tmp88EB.tmp'
Imagebase:	0xe20000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp88EB.tmp	unknown	2	success or wait	1	E2AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp88EB.tmp	unknown	1641	success or wait	1	E2ABD9	ReadFile

Analysis Process: conhost.exe PID: 6612 Parent PID: 6604

General

Start time:	12:36:18
Start date:	20/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: .exe PID: 6752 Parent PID: 6444

General

Start time:	12:36:19
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\ .exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x510000
File size:	561664 bytes
MD5 hash:	4C0960A22153523B2626BFF364CC7073
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: 00000004.00000002.475265979.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.478164785.0000000002931000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.478164785.0000000002931000.00000004.00000001.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	6E12CF06	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	6E12CF06	unknown
C:\Users\user\AppData\Roaming\51qhj2rq.aji	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF7BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\51qhj2rq.aji\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF7BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\51qhj2rq.aji\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF7BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\51qhj2rq.aji\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CF7DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\51qhj2rq.aji\Chrome\Default\Cookies	success or wait	1	6CF76A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\51qhj2rq.aji\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6CF7DD66	CopyFileW

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	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E105705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E10CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E105705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF71B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CF71B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CF71B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF71B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CF71B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\466c55ec-057b-42e9-8980-2452ccc22e9e	unknown	4096	success or wait	1	6CF71B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CF71B4F	ReadFile
C:\Users\user\AppData\Roaming\51qhj2rq.aji\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CF71B4F	ReadFile

Disassembly

Code Analysis