ID: 344975
Sample Name: njGJ1eW44wshoMr.exe
Cookbook: default.jbs
Time: 15:16:14
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

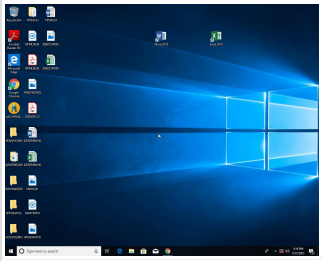
Analysis Report njGJ1eW44wshoMr.exe

Overview

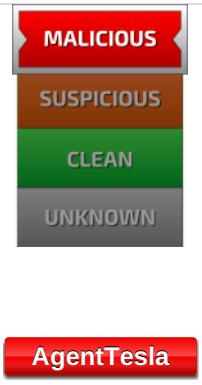
General Information

Sample Name:	njGJ1eW44wshoMr.exe
Analysis ID:	344975
MD5:	3642d5bf033629d.
SHA1:	47993d2f980a7c3.
SHA256:	c7af68bcec3b1c2..
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection



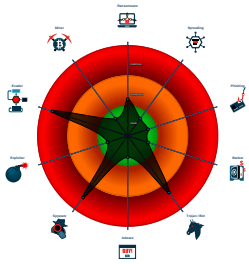
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…

Classification



Startup

- **System is w10x64**
- njGJ1eW44wshoMr.exe (PID: 4188 cmdline: 'C:\Users\user\Desktop\njGJ1eW44wshoMr.exe' MD5: 3642D5BF033629D0A716FFF2C17125B2)
  - njGJ1eW44wshoMr.exe (PID: 6468 cmdline: {path} MD5: 3642D5BF033629D0A716FFF2C17125B2)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "Msrcg53Go53k",
  "URL: ": "http://u8XlnFfKOIQs9ntdu.org",
  "To: ": "presidencia@cefortem.cat",
  "ByHost: ": "mail.cefortem.cat:587",
  "Password: ": "4RubS",
  "From: ": "presidencia@cefortem.cat"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.680815845.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.355060435.0000000003E90000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.354112729.0000000002DD7000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000002.683036649.0000000002BE1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.683036649.0000000002BE1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 4 entries				

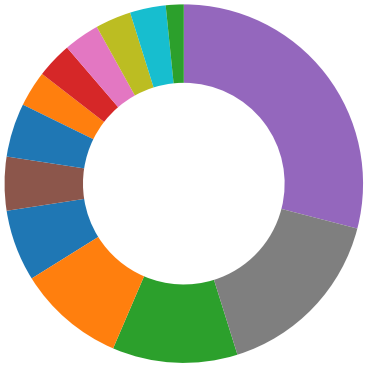
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.njGJ1eW44wshoMr.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

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

Networking:

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Data Obfuscation:

.NET source code contains potential unpacker

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)

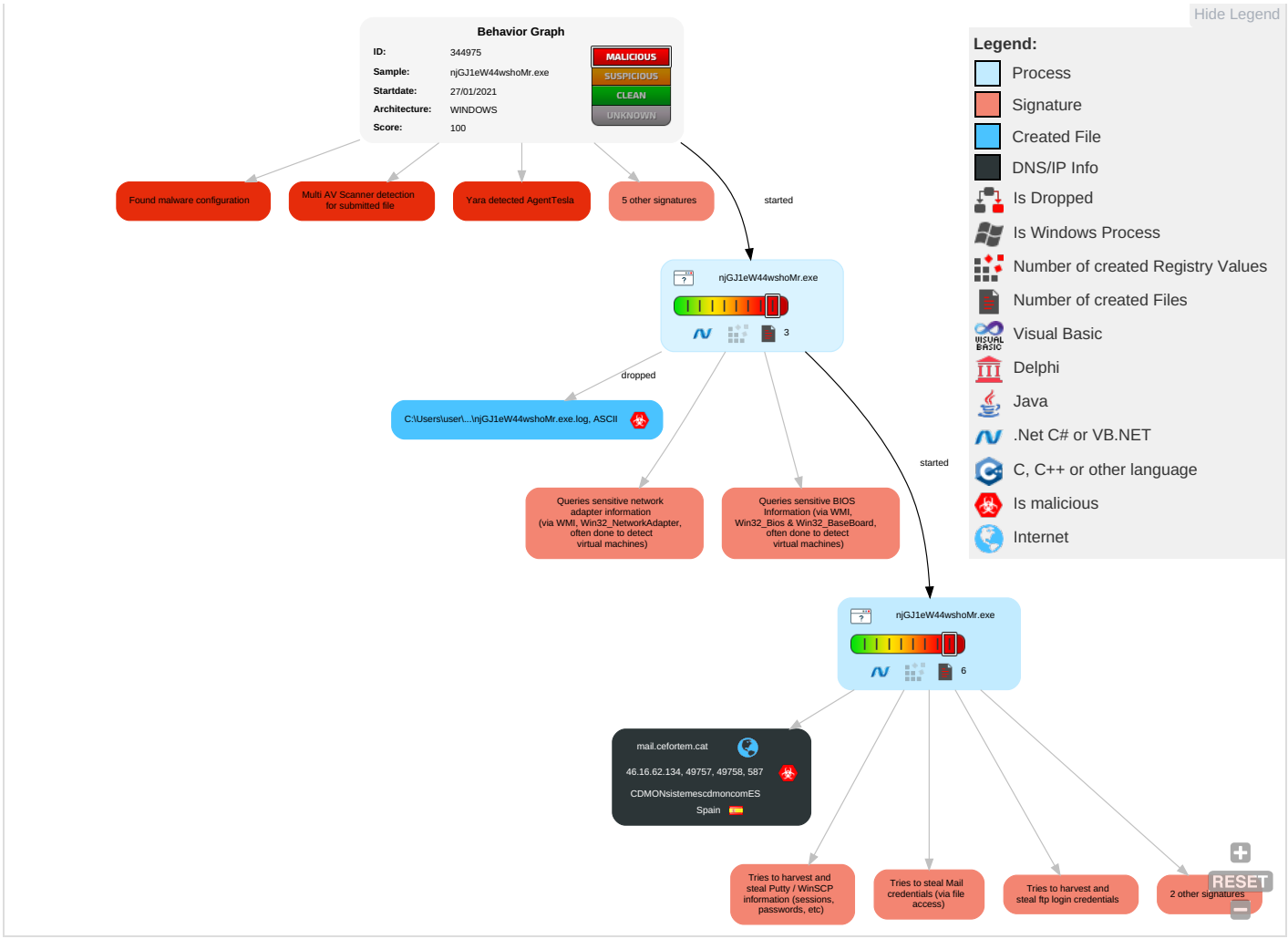
Remote Access Functionality:

- 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	Path Interception	Process Injection 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 2	Input Capture 1 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 1 2	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Application Layer Protocol 1 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 3	LSA Secrets	Virtualization/Sandbox Evasion 1 3	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 Us Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application La Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocol

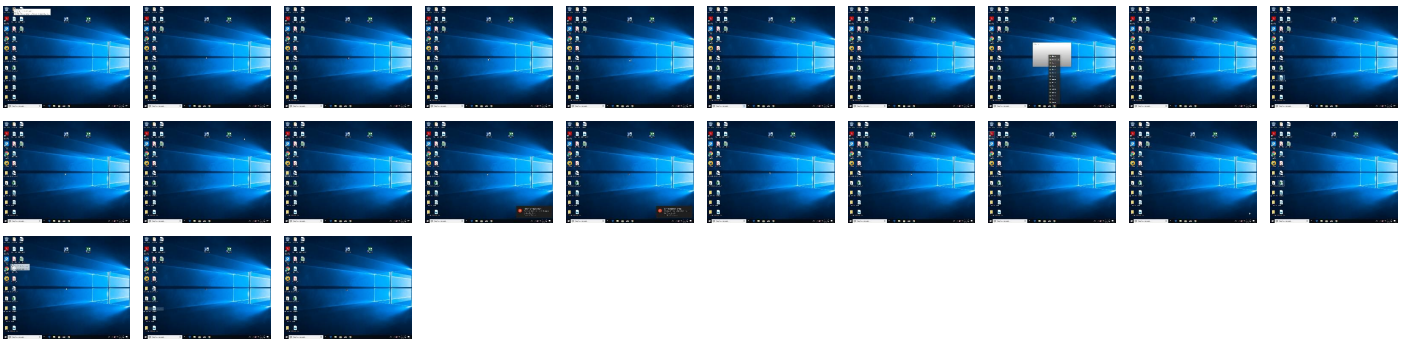
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
njGJ1eW44wshoMr.exe	26%	Virustotal		Browse
njGJ1eW44wshoMr.exe	30%	ReversingLabs	ByteCode-MSIL.Packed.Generic	
njGJ1eW44wshoMr.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.njGJ1eW44wshoMr.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.carterandcone.comofG	0%	Avira URL Cloud	safe	
http://DXhCun.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sandoll.co.kr6	0%	Avira URL Cloud	safe	
http://www.carterandcone.comes	0%	Avira URL Cloud	safe	
http://www.carterandcone.comva	0%	Avira URL Cloud	safe	
http://www.carterandcone.comen	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnark	0%	Avira URL Cloud	safe	
http://r3.i.lencr	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.zhongyicts.com.cnofG	0%	Avira URL Cloud	safe	
http://www.carterandcone.comkO	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com-	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://www.founder.com.cn/cnD	0%	Avira URL Cloud	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.fontbureau.comas	0%	Avira URL Cloud	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.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comr-tk	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html&	0%	Avira URL Cloud	safe	
http://www.carterandcone.comO	0%	Avira URL Cloud	safe	
http://www.sandoll.cn	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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://fontfabrik.comh	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://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	
http://www.sandoll.co.krs-cl	0%	Avira URL Cloud	safe	
http://www.carterandcone.comue-	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://u8XlnFfKOIQs9ntdu.org	0%	Avira URL Cloud	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.comexc	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://www.carterandcone.comf	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/7	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.cefortem.cat	46.16.62.134	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://u8XlnFfKOIQs9ntdu.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	njGJ1eW44wshoMr.exe, 00000001.00000002.683036649.0000000002BE1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.comofG	njGJ1eW44wshoMr.exe, 00000000.00000003.335917362.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false		high
http://DXhCun.com	njGJ1eW44wshoMr.exe, 00000001.00000002.683036649.0000000002BE1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

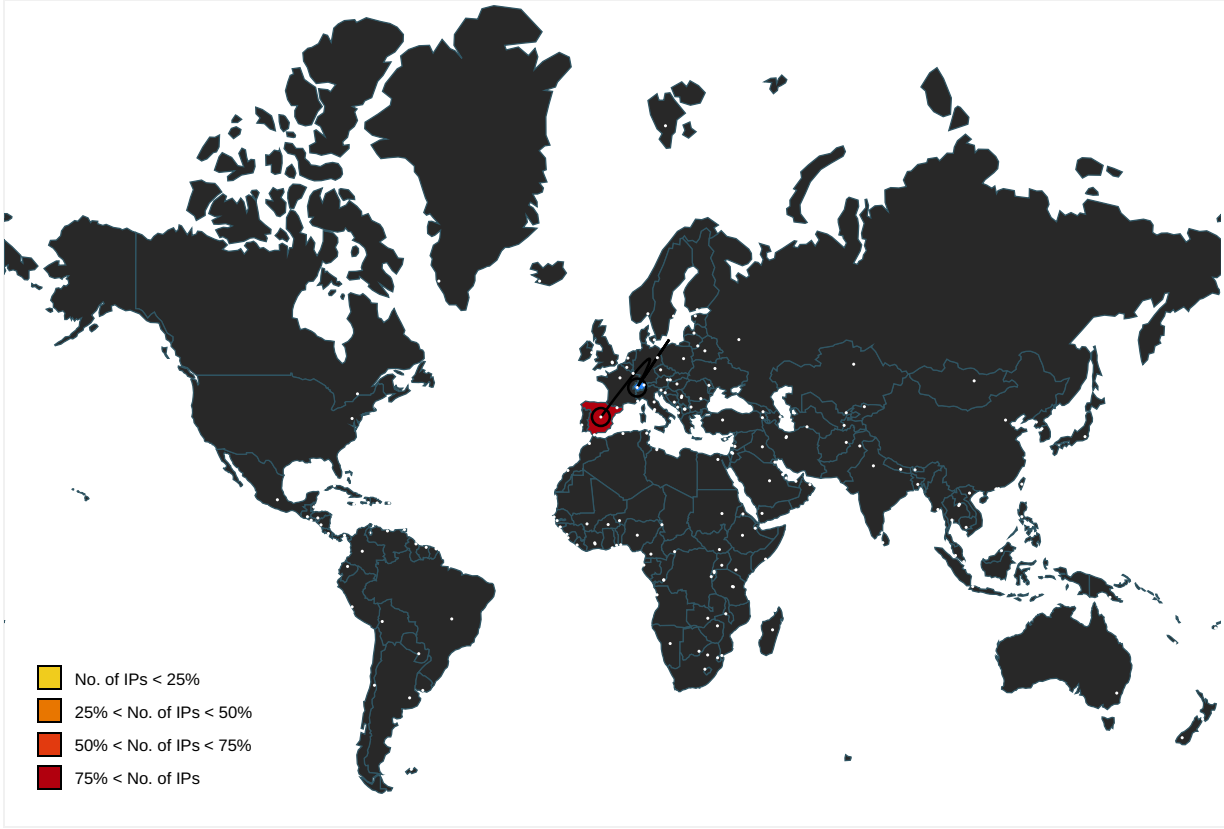
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersL	njGJ1eW44wshoMr.exe, 00000000.00000003.339605314.0000000005D7B000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.kr6	njGJ1eW44wshoMr.exe, 00000000.00000003.333676360.0000000005D7F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comes	njGJ1eW44wshoMr.exe, 00000000.00000003.336266777.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comva	njGJ1eW44wshoMr.exe, 00000000.00000003.335917362.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comen	njGJ1eW44wshoMr.exe, 00000000.00000003.336266777.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersB	njGJ1eW44wshoMr.exe, 00000000.00000003.344524376.0000000005D7B000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnark	njGJ1eW44wshoMr.exe, 00000000.00000003.334704774.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.i.lencr	njGJ1eW44wshoMr.exe, 00000001.00000002.682596949.0000000011170000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cnofG	njGJ1eW44wshoMr.exe, 00000000.00000003.335064386.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comkO	njGJ1eW44wshoMr.exe, 00000000.00000003.335917362.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp, njGJ1eW44wshoMr.exe, 00000000.00000003.344524376.0000000005D7B000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/O	njGJ1eW44wshoMr.exe, 00000000.00000003.339182936.0000000005D7B000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	njGJ1eW44wshoMr.exe, 00000000.00000003.333676360.0000000005D7F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	njGJ1eW44wshoMr.exe, 00000000.00000003.336631403.0000000005D7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersO	njGJ1eW44wshoMr.exe, 00000000.00000003.339605314.0000000005D7B000.00000004.00000001.sdmp	false		high
http://www.carterandcone.com-	njGJ1eW44wshoMr.exe, 00000000.00000003.335917362.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://r3.i.lencr.org/0	njGJ1eW44wshoMr.exe, 00000001.00000002.687782985.0000000005F6C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnD	njGJ1eW44wshoMr.exe, 00000000.00000003.334128429.0000000005D84000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	njGJ1eW44wshoMr.exe, 00000000.00000003.331736060.0000000005D62000.00000004.00000001.sdmp, njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comas	njGJ1eW44wshoMr.exe, 00000000.00000002.354020205.00000000014F7000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/cThe	njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	njGJ1eW44wshoMr.exe, 00000000.00000003.342253941.0000000005D7B000.00000004.00000001.sdmp, njGJ1eW44wshoMr.exe, 00000000.00000003.342086297.0000000005D7B000.00000004.00000001.sdmp, njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	njGJ1eW44wshoMr.exe, 00000000.00000003.332609376.0000000005D7B000.00000004.00000001.sdmp, njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.htmlG	njGJ1eW44wshoMr.exe, 00000000.00000003.339875376.0000000005D7B000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comC	njGJ1eW44wshoMr.exe, 00000000.00000003.335917362.0000000005D7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersa	njGJ1eW44wshoMr.exe, 00000000.00000003.339557174.0000000005D7B000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comr-tk	njGJ1eW44wshoMr.exe, 00000000.00000003.335917362.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.o.lencr.org0	njGJ1eW44wshoMr.exe, 00000001.00000002.687782985.0000000005F6C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	njGJ1eW44wshoMr.exe, 00000001.00000002.683036649.0000000002BE1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.ascendercorp.com/typedesigners.html	njGJ1eW44wshoMr.exe, 00000000.00000003.337317423.0000000005D83000.00000004.00000001.sdmp, njGJ1eW44wshoMr.exe, 00000000.00000003.337240657.0000000005D83000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html&	njGJ1eW44wshoMr.exe, 00000000.00000003.337279867.0000000005D83000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comO	njGJ1eW44wshoMr.exe, 00000000.00000003.336266777.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false		high
http://www.sandoll.cn	njGJ1eW44wshoMr.exe, 00000000.00000003.333749487.0000000005D7F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr	njGJ1eW44wshoMr.exe, 00000000.00000003.333676360.0000000005D7F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.comh	njGJ1eW44wshoMr.exe, 00000000.00000003.332609376.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersz	njGJ1eW44wshoMr.exe, 00000000.00000003.339706590.0000000005D7B000.00000004.00000001.sdmp, njGJ1eW44wshoMr.exe, 00000000.00000003.339651663.0000000005D7B000.00000004.00000001.sdmp	false		high
http://www.urwpp.de	njGJ1eW44wshoMr.exe, 00000000.00000003.339035591.0000000005D7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	njGJ1eW44wshoMr.exe, 00000000.00000003.335498649.0000000005D7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false	• 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	njGJ1eW44wshoMr.exe, 00000000.00000002.355060435.0000000003E90000.00000004.00000001.sdmp, njGJ1eW44wshoMr.exe, 00000001.00000002.680815845.0000000004402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krs-cl	njGJ1eW44wshoMr.exe, 00000000.00000003.333676360.0000000005D7F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comue-	njGJ1eW44wshoMr.exe, 00000000.00000003.336266777.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://cps.root-x1.letsencrypt.org0	njGJ1eW44wshoMr.exe, 00000001.00000002.687782985.0000000005F6C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coma	njGJ1eW44wshoMr.exe, 00000000.00000003.335498649.0000000005D7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comexc	njGJ1eW44wshoMr.exe, 00000000.00000003.335498649.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com	njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	njGJ1eW44wshoMr.exe, 00000001.00000002.683036649.0000000002BE1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comf	njGJ1eW44wshoMr.exe, 00000000.00000003.335917362.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/7	njGJ1eW44wshoMr.exe, 00000000.00000003.333749487.0000000005D7F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comt	njGJ1eW44wshoMr.exe, 00000000.00000003.331736060.0000000005D62000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.m.	njGJ1eW44wshoMr.exe, 00000000.00000003.333347958.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.letsencrypt.org0	njGJ1eW44wshoMr.exe, 00000001.00000002.687782985.0000000005F6C000.00000004.00000001.sdmp	false	• 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	njGJ1eW44wshoMr.exe, 00000001.00000002.683036649.0000000002BE1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comfac	njGJ1eW44wshoMr.exe, 00000000.00000003.335213930.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.como.M	njGJ1eW44wshoMr.exe, 00000000.00000003.335917362.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comslnt	njGJ1eW44wshoMr.exe, 00000000.00000003.335917362.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.w	njGJ1eW44wshoMr.exe, 00000000.00000003.332863380.0000000005D7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comn	njGJ1eW44wshoMr.exe, 00000000.00000003.335917362.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%$	njGJ1eW44wshoMr.exe, 00000001.00000002.683036649.0000000002BE1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deC	njGJ1eW44wshoMr.exe, 00000000.00000003.339035591.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/	njGJ1eW44wshoMr.exe, 00000000.00000003.334385567.0000000005D7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	njGJ1eW44wshoMr.exe, 00000000.00000003.334128429.0000000005D84000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	njGJ1eW44wshoMr.exe, 00000000.00000003.340038806.0000000005D9E000.00000004.00000001.sdmp, njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false		high
http://www.tiro.comn-u	njGJ1eW44wshoMr.exe, 00000000.00000003.334654620.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	njGJ1eW44wshoMr.exe, 00000000.00000003.342211762.0000000005D9E000.00000004.00000001.sdmp, njGJ1eW44wshoMr.exe, 00000000.00000003.340409954.0000000005D9E000.00000004.00000001.sdmp	false		high
http://www.tiro.comT	njGJ1eW44wshoMr.exe, 00000000.00000003.336110347.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnZ	njGJ1eW44wshoMr.exe, 00000000.00000003.335064386.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cno.	njGJ1eW44wshoMr.exe, 00000000.00000003.336631403.0000000005D7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.cefortem.cat	njGJ1eW44wshoMr.exe, 00000001.00000002.684619940.0000000002F4D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	njGJ1eW44wshoMr.exe, 00000000.00000003.340685503.0000000005D7B000.00000004.00000001.sdmp, njGJ1eW44wshoMr.exe, 00000000.00000002.358220825.0000000005E50000.00000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cnO	njGJ1eW44wshoMr.exe, 00000000.00000003.335064386.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnl-sM	njGJ1eW44wshoMr.exe, 00000000.00000003.334801239.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comf	njGJ1eW44wshoMr.exe, 00000000.00000003.336266777.0000000005D7B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com9t	njGJ1eW44wshoMr.exe, 00000000.00000002.354020205.00000000014F7000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
46.16.62.134	unknown	Spain		197712	CDMONsistemescdmoncom ES	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344975
Start date:	27.01.2021
Start time:	15:16:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	njGJ1eW44wshoMr.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:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/2@2/1

EGA Information:	Failed
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:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 13.64.90.137, 52.147.198.201, 51.104.139.180, 95.101.22.216, 95.101.22.224, 52.155.217.156, 20.54.26.129, 67.27.159.126, 8.248.139.254, 67.27.158.126, 67.27.157.254, 67.27.158.254, 51.103.5.186, 51.104.144.132, 23.210.248.85 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net, vip2-par02p.wns.notify.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
15:17:12	API Interceptor	1044x Sleep call for process: njGJ1eW44wshoMr.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
46.16.62.134	3nG9LW7Z21dxUoM.exe	Get hash	malicious	Browse	
	keeFDE9dhCGNNez.exe	Get hash	malicious	Browse	
	74tF1foMeQyUMCh.exe	Get hash	malicious	Browse	
	qm7JU84PFgfqvgs.exe	Get hash	malicious	Browse	
	WbGKi8E5OE4eCFG.exe	Get hash	malicious	Browse	
	r9SWnqQlK8PFPEp.exe	Get hash	malicious	Browse	
	L9oOm9x3l7YZFcA.exe	Get hash	malicious	Browse	
	jKiL1mzTAVltJ30.exe	Get hash	malicious	Browse	
	09xcuRN2HJmRRCm.exe	Get hash	malicious	Browse	
	aLjBjGUvWecwGptNRQryBtRBaVCtO.exe	Get hash	malicious	Browse	
	UsU2f18QuIdAe2U.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.cefortem.cat	3nG9LW7Z21dxUoM.exe	Get hash	malicious	Browse	• 46.16.62.134
	keeFDE9dhCGNNez.exe	Get hash	malicious	Browse	• 46.16.62.134
	74tF1foMeQyUMCh.exe	Get hash	malicious	Browse	• 46.16.62.134
	qm7JU84PFgfqvgs.exe	Get hash	malicious	Browse	• 46.16.62.134
	WbGKi8E5OE4eCFG.exe	Get hash	malicious	Browse	• 46.16.62.134
	r9SWnqQlK8PFPEp.exe	Get hash	malicious	Browse	• 46.16.62.134
	L9oOm9x3l7YZFcA.exe	Get hash	malicious	Browse	• 46.16.62.134
	jKiL1mzTAVltJ30.exe	Get hash	malicious	Browse	• 46.16.62.134
	09xcuRN2HJmRRCm.exe	Get hash	malicious	Browse	• 46.16.62.134
	aLjBjGUvWecwGptNRQryBtRBaVCtO.exe	Get hash	malicious	Browse	• 46.16.62.134
	UsU2f18QuIdAe2U.exe	Get hash	malicious	Browse	• 46.16.62.134

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CDMONsistemescdmoncomES	3nG9LW7Z21dxUoM.exe	Get hash	malicious	Browse	• 46.16.62.134
	keeFDE9dhCGNNez.exe	Get hash	malicious	Browse	• 46.16.62.134
	74tF1foMeQyUMCh.exe	Get hash	malicious	Browse	• 46.16.62.134
	qm7JU84PFgfqvgs.exe	Get hash	malicious	Browse	• 46.16.62.134
	winlog.exe	Get hash	malicious	Browse	• 46.16.61.250
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 46.16.61.250
	WbGKi8E5OE4eCFG.exe	Get hash	malicious	Browse	• 46.16.62.134
	r9SWnqQlK8PFPEp.exe	Get hash	malicious	Browse	• 46.16.62.134
	L9oOm9x3l7YZFcA.exe	Get hash	malicious	Browse	• 46.16.62.134
	SecuriteInfo.com.Trojan.DownLoader36.34557.26355.exe	Get hash	malicious	Browse	• 134.0.10.35
	jKiL1mzTAVltJ30.exe	Get hash	malicious	Browse	• 46.16.62.134
	09xcuRN2HJmRRCm.exe	Get hash	malicious	Browse	• 46.16.62.134
	57229937-122020-4-7676523.doc	Get hash	malicious	Browse	• 185.66.41.128
	aLjBjGUvWecwGptNRQryBtRBaVCtO.exe	Get hash	malicious	Browse	• 46.16.62.134
	UsU2f18QuIdAe2U.exe	Get hash	malicious	Browse	• 46.16.62.134
	Nakit Akisi Detaylariniz.exe	Get hash	malicious	Browse	• 46.16.61.250
	Archivo_122020_1977149.doc	Get hash	malicious	Browse	• 185.66.41.128
	Doc.doc	Get hash	malicious	Browse	• 185.66.41.127
	JI35907_2020.doc	Get hash	malicious	Browse	• 185.66.41.127
	SHIPMENT DOCUMENTS, INV+BL DRAFT.exe	Get hash	malicious	Browse	• 185.34.194.66

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\njGJ1eW44wshoMr.exe.log	
Process:	C:\Users\user\Desktop\njGJ1eW44wshoMr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, 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\Roaming\y2hqe4dr.iim\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\njGJ1eW44wshoMr.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6951152985249047
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBopIvJn2QOYiUG3PaVrX:T5LLOpEO5J/Kn7U1uBopIvZXC/alX
MD5:	EA7F9615D77815B5FFF7C15179C6C560
SHA1:	3D1D0BAC6633344E2B6592464EBB957D0D8DD48F
SHA-256:	A5D1ABB57C516F4B3DF3D18950AD1319BA1A63F9A39785F8F0EACE0A482CAB17
SHA-512:	9C818471F69758BD4884FDB9B543211C9E1EE832AC29C2C5A0377C412454E8C745FB3F38FF6E3853AE365D04933C0EC55A46DDA60580D244B308F92C57258C98
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.38324091168724
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	njGJ1eW44wshoMr.exe
File size:	832000
MD5:	3642d5bf033629d0a716fff2c17125b2
SHA1:	47993d2f980a7c3de204b008618c9b4c25511a49
SHA256:	c7af68bcec3b1c2e3a87f08111ab75b525799c5386fa85b529f8690bfa1c766a
SHA512:	d0539565dbd492ed31b00accab13a629f2535fe9d3123e90038fb55591a079d9ddc0e9f7fde493cdb49621f50901283e0d8a8343617089519b0cac57b9eda4d0
SSDEEP:	12288:Gqfu19QFt3oLWPaoMeSEKBtqKuCwaBjaBF:Ggt3oLiMeSTBtq9Za1a

General

File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......PE..L..... .`..............0.................. ....@.. .... @................................

File Icon

	
Icon Hash:	e0dc9e0e1e9296e8

Static PE Info

General

Entrypoint:	0x4bbdce
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:	0x6010D3C4 [Wed Jan 27 02:45:24 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbbd7c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbc000	0x10e98	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xce000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb9dd4	0xb9e00	False	0.643945443847	data	7.54334100572	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbc000	0x10e98	0x11000	False	0.133128446691	data	4.50774411316	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xce000	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	0xbc100	0x10828	data		
RT_GROUP_ICON	0xcc938	0x14	data		
RT_VERSION	0xcc95c	0x33c	data		
RT_MANIFEST	0xccca8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

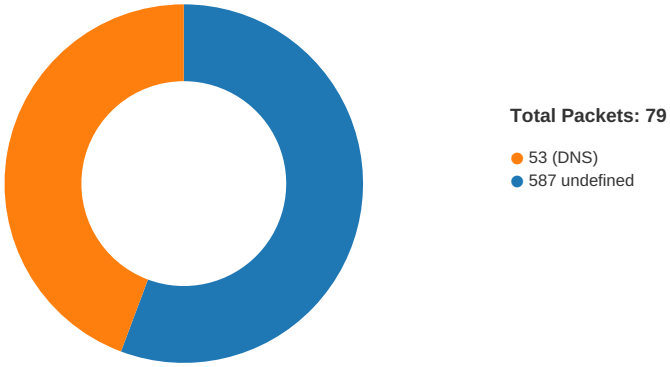
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	Zwj.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	HotelMgmtSystem
ProductVersion	1.0.0.0
FileDescription	HotelMgmtSystem
OriginalFilename	Zwj.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:18:58.971848965 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:18:59.033337116 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:18:59.033540964 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:18:59.679548979 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:18:59.680159092 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:18:59.739547014 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:18:59.739764929 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:18:59.740308046 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:18:59.800381899 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:18:59.850013018 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:18:59.881191969 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:18:59.946923018 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:18:59.946962118 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:18:59.946980000 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:18:59.947123051 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:18:59.958525896 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:00.020937920 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:00.068723917 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:00.531128883 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:00.590985060 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:00.593214035 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:00.652664900 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:00.654033899 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:00.719590902 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:00.721302032 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:00.785753012 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:00.786225080 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:00.852276087 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:00.852926016 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:00.913556099 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:00.916759014 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:00.916860104 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:00.917643070 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:00.917711020 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:00.976367950 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:00.980758905 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:01.068741083 CET	587	49757	46.16.62.134	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:19:01.115701914 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:03.480679035 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:03.543390036 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:03.543489933 CET	587	49757	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:03.543580055 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:03.673533916 CET	49757	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.057267904 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.116765022 CET	587	49758	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:04.119281054 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.213311911 CET	587	49758	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:04.213740110 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.274231911 CET	587	49758	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:04.274247885 CET	587	49758	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:04.274631977 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.334006071 CET	587	49758	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:04.334525108 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.397619009 CET	587	49758	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:04.399039984 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.399627924 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.461936951 CET	587	49758	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:04.461961031 CET	587	49758	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:04.462543011 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.522383928 CET	587	49758	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:04.523814917 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.587853909 CET	587	49758	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:04.588437080 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.649934053 CET	587	49758	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:04.650512934 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.715550900 CET	587	49758	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:04.715950966 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.778768063 CET	587	49758	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:04.781414032 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.781725883 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.781898975 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.782078981 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.782417059 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.782530069 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.782634974 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.782751083 CET	49758	587	192.168.2.6	46.16.62.134
Jan 27, 2021 15:19:04.843467951 CET	587	49758	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:04.843492985 CET	587	49758	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:04.845757961 CET	587	49758	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:05.941018105 CET	587	49758	46.16.62.134	192.168.2.6
Jan 27, 2021 15:19:05.991224051 CET	49758	587	192.168.2.6	46.16.62.134

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:16:59.815766096 CET	58384	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:16:59.866231918 CET	53	58384	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:00.783004045 CET	60261	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:00.830945015 CET	53	60261	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:01.711787939 CET	56061	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:01.759639025 CET	53	56061	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:02.708695889 CET	58336	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:02.759476900 CET	53	58336	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:05.516943932 CET	53781	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:05.566940069 CET	53	53781	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:06.833964109 CET	54064	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:06.884680986 CET	53	54064	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:08.478435040 CET	52811	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:08.529804945 CET	53	52811	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:09.690593004 CET	55299	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:09.753953934 CET	53	55299	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:17:10.515866041 CET	63745	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:10.566662073 CET	53	63745	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:11.341995001 CET	50055	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:11.389877081 CET	53	50055	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:12.467647076 CET	61374	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:12.518620014 CET	53	61374	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:13.326427937 CET	50339	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:13.374473095 CET	53	50339	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:14.084614992 CET	63307	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:14.132606983 CET	53	63307	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:27.842717886 CET	49694	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:27.896604061 CET	53	49694	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:32.180165052 CET	54982	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:32.238857031 CET	53	54982	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:46.335989952 CET	50010	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:46.396779060 CET	53	50010	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:47.063313007 CET	63718	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:47.122426033 CET	53	63718	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:47.704229116 CET	62116	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:47.762708902 CET	53	62116	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:47.854887009 CET	63816	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:47.905693054 CET	53	63816	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:48.209753036 CET	55014	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:48.269081116 CET	53	55014	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:48.772367001 CET	62208	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:48.831435919 CET	53	62208	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:49.102900982 CET	57574	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:49.151017904 CET	53	57574	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:49.383307934 CET	51818	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:49.444660902 CET	53	51818	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:49.568905115 CET	56628	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:49.616848946 CET	53	56628	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:50.049755096 CET	60778	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:50.106091976 CET	53	60778	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:50.975233078 CET	53799	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:51.028278112 CET	53	53799	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:52.093208075 CET	54683	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:52.141129017 CET	53	54683	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:52.656398058 CET	59329	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:52.704351902 CET	53	59329	8.8.8.8	192.168.2.6
Jan 27, 2021 15:17:54.047588110 CET	64021	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:17:54.108644009 CET	53	64021	8.8.8.8	192.168.2.6
Jan 27, 2021 15:18:29.896775961 CET	56129	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:18:29.944745064 CET	53	56129	8.8.8.8	192.168.2.6
Jan 27, 2021 15:18:35.059742928 CET	58177	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:18:35.122203112 CET	53	58177	8.8.8.8	192.168.2.6
Jan 27, 2021 15:18:54.687736988 CET	50700	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:18:54.736819983 CET	53	50700	8.8.8.8	192.168.2.6
Jan 27, 2021 15:18:55.164331913 CET	54069	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:18:55.215059042 CET	53	54069	8.8.8.8	192.168.2.6
Jan 27, 2021 15:18:58.776926994 CET	61178	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:18:58.866444111 CET	53	61178	8.8.8.8	192.168.2.6
Jan 27, 2021 15:19:03.998423100 CET	57017	53	192.168.2.6	8.8.8.8
Jan 27, 2021 15:19:04.054814100 CET	53	57017	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 15:18:58.776926994 CET	192.168.2.6	8.8.8.8	0x7864	Standard query (0)	mail.cefortem.cat	A (IP address)	IN (0x0001)
Jan 27, 2021 15:19:03.998423100 CET	192.168.2.6	8.8.8.8	0x6cbf	Standard query (0)	mail.cefortem.cat	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:18:58.866444111 CET	8.8.8.8	192.168.2.6	0x7864	No error (0)	mail.cefortem.cat		46.16.62.134	A (IP address)	IN (0x0001)
Jan 27, 2021 15:19:04.054814100 CET	8.8.8.8	192.168.2.6	0x6cbf	No error (0)	mail.cefortem.cat		46.16.62.134	A (IP address)	IN (0x0001)

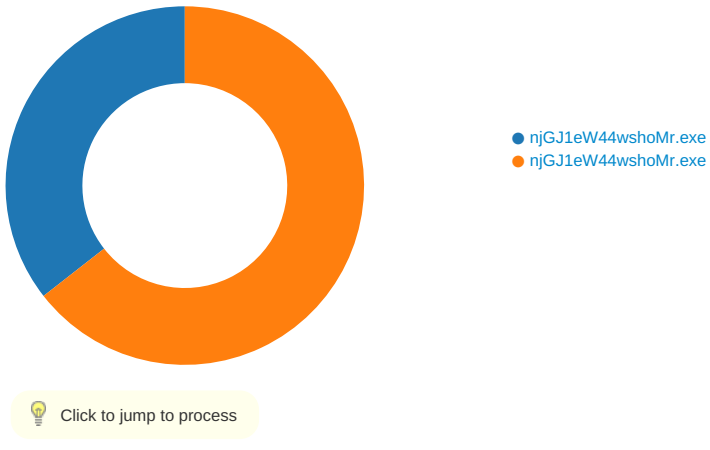
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 15:18:59.679548979 CET	587	49757	46.16.62.134	192.168.2.6	220 fnadk-03.srv.cat ESMTP
Jan 27, 2021 15:18:59.680159092 CET	49757	587	192.168.2.6	46.16.62.134	EHLO 642294
Jan 27, 2021 15:18:59.739764929 CET	587	49757	46.16.62.134	192.168.2.6	250-fnadk-03.srv.cat 250-PIPELINING 250-SIZE 47185920 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN CRAM-MD5 DIGEST-MD5 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Jan 27, 2021 15:18:59.740308046 CET	49757	587	192.168.2.6	46.16.62.134	STARTTLS
Jan 27, 2021 15:18:59.800381899 CET	587	49757	46.16.62.134	192.168.2.6	220 2.0.0 Ready to start TLS
Jan 27, 2021 15:19:04.213311911 CET	587	49758	46.16.62.134	192.168.2.6	220 fnadk-03.srv.cat ESMTP
Jan 27, 2021 15:19:04.213740110 CET	49758	587	192.168.2.6	46.16.62.134	EHLO 642294
Jan 27, 2021 15:19:04.274247885 CET	587	49758	46.16.62.134	192.168.2.6	250-fnadk-03.srv.cat 250-PIPELINING 250-SIZE 47185920 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN CRAM-MD5 DIGEST-MD5 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Jan 27, 2021 15:19:04.274631977 CET	49758	587	192.168.2.6	46.16.62.134	STARTTLS
Jan 27, 2021 15:19:04.334006071 CET	587	49758	46.16.62.134	192.168.2.6	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: njGJ1eW44wshoMr.exe PID: 4188 Parent PID: 5984

General

Start time:	15:17:04
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\njGJ1eW44wshoMr.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\njGJ1eW44wshoMr.exe'
Imagebase:	0x9c0000
File size:	832000 bytes
MD5 hash:	3642D5BF033629D0A716FFF2C17125B2
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: 00000000.00000002.355060435.0000000003E90000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.354112729.0000000002DD7000.00000004.00000001.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	6DFFCF06	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	6DFFCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\njGJ1eW44wshoMr.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E30C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\njGJ1eW44wshoMr.exe.log	unknown	1216	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	6E30C907	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	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	ReadFile

Analysis Process: njGJ1eW44wshoMr.exe PID: 6468 Parent PID: 4188

General

Start time:	15:17:15
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\njGJ1eW44wshoMr.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x7b0000
File size:	832000 bytes
MD5 hash:	3642D5BF033629D0A716FFF2C17125B2
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.680815845.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.683036649.0000000002BE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.683036649.0000000002BE1000.00000004.00000001.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	6DFFCF06	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	6DFFCF06	unknown
C:\Users\user\AppData\Roaming\y2hqe4dr.iim	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CE4BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\y2hqe4dr.iim\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	6CE4BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\y2hqe4dr.iim\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	6CE4BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\y2hqe4dr.iim\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	6CE4DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\y2hqe4dr.iim\Chrome\Default\Cookies	success or wait	1	6CE46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\y2hqe4dr.iim\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 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	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6CE4DD66	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	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\e68b830e-2a06-4a09-aa6a-9e8e3854865e	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6CE41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Roaming\y2hqe4dr.iim\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CE41B4F	ReadFile

Disassembly

Code Analysis

Code Analysis