ID: 404247
Sample Name:
7XCBqj5HLqHcRlU.exe
Cookbook: default.jbs
Time: 20:44:58
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

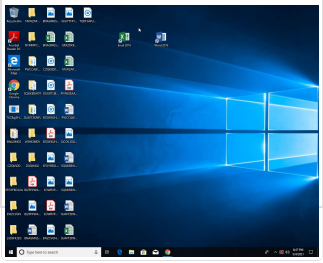
Analysis Report 7XCBqj5HLqHcRlU.exe

Overview

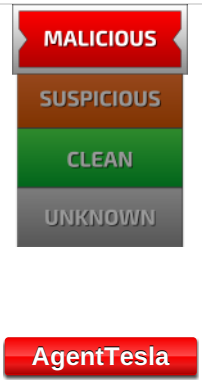
General Information

Sample Name:	7XCBqj5HLqHcRlU.exe
Analysis ID:	404247
MD5:	09a25586d2eaf5e.
SHA1:	33acc64a84386fc..
SHA256:	e34725603d4f017.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

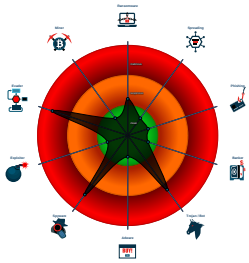


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- 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**
- 7XCBqj5HLqHcRlU.exe (PID: 5452 cmdline: 'C:\Users\user\Desktop\7XCBqj5HLqHcRlU.exe' MD5: 09A25586D2EAF5E8C3A5DF5557BAD218)
  - 7XCBqj5HLqHcRlU.exe (PID: 5628 cmdline: {path} MD5: 09A25586D2EAF5E8C3A5DF5557BAD218)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "security@prisamexico.netOpy44Yi.e65ymail.prisamexico.net"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.471184243.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.241704135.0000000003DFF000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.476530485.0000000002A01000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: 7XCBqj5HLqHcRlU.exe PID: 5628	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: 7XCBqj5HLqHcRlU.exe PID: 5628	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 2 entries

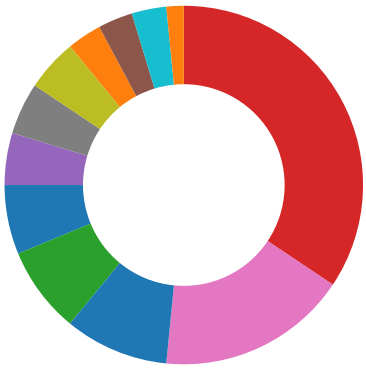
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.7XCBqj5HLqHcRlU.exe.3ea1480.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.7XCBqj5HLqHcRlU.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.7XCBqj5HLqHcRlU.exe.3ea1480.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Networking
- 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

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Yara detected AntiVM3

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)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

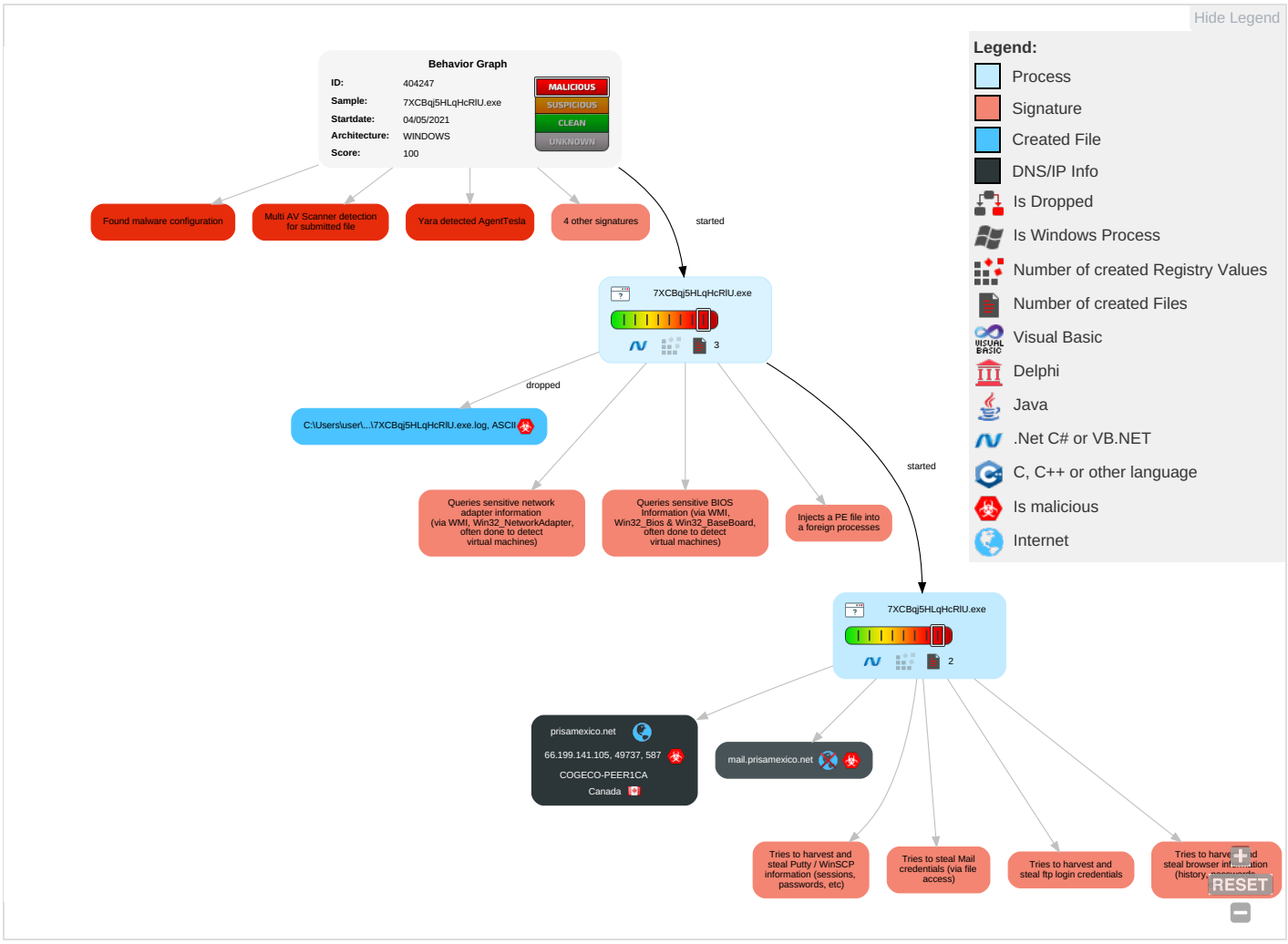
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

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

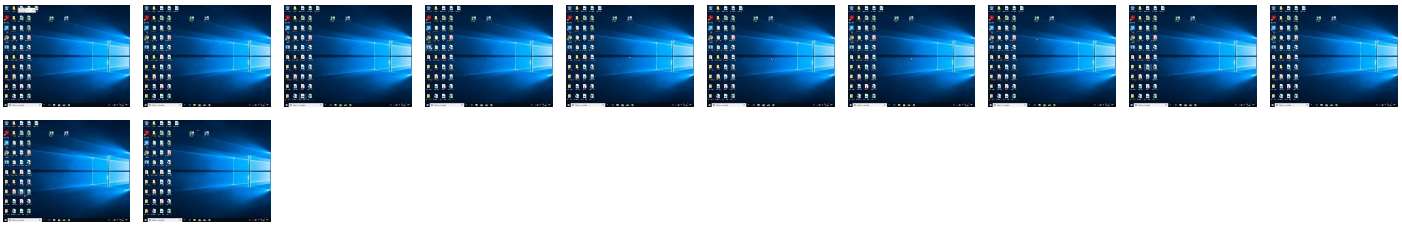
Behavior Graph



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
7XCBqj5HLqHcRlU.exe	21%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
7XCBqj5HLqHcRlU.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.7XCBqj5HLqHcRlU.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	

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	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://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	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://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.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://prisamexico.net	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://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.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://mail.prisamexico.net	0%	Avira URL Cloud	safe	
http://yjaeXK8No5PRZuzN.net	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://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://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://hDgEgh.com	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.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://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	

Domains and IPs

Contacted Domains

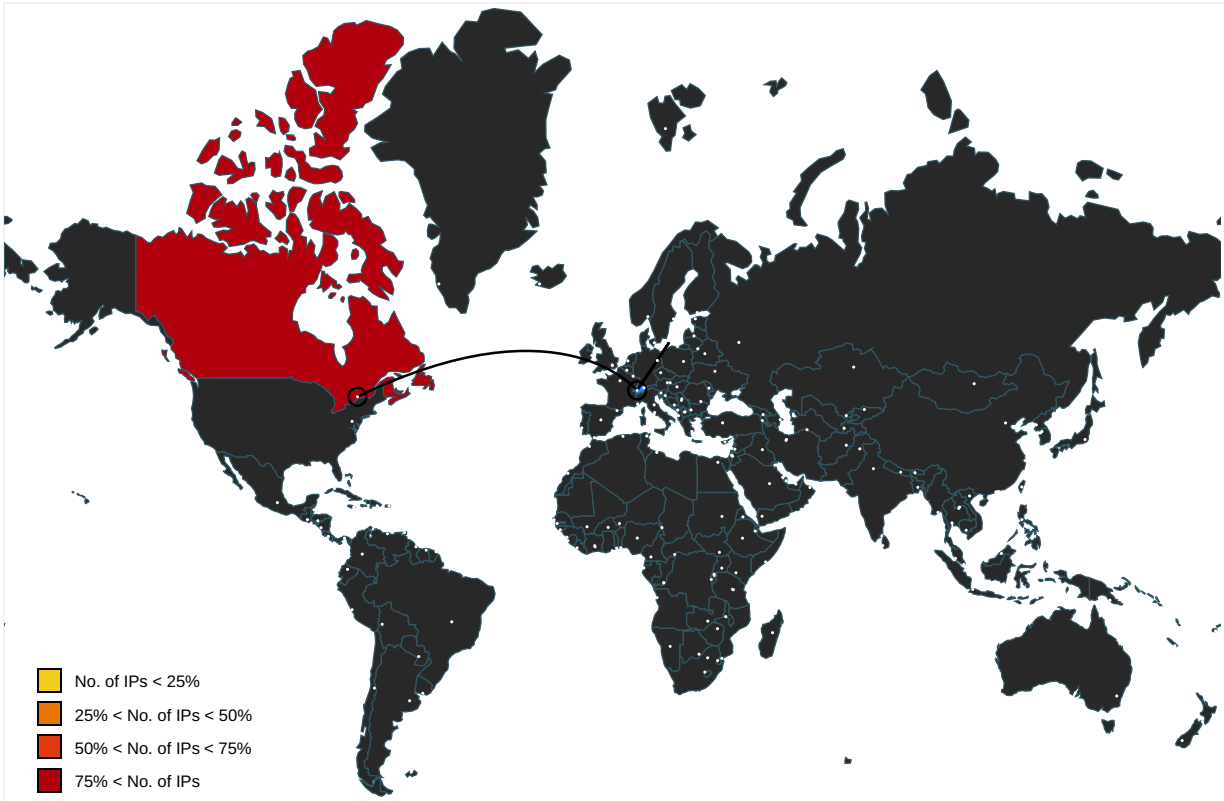
Name	IP	Active	Malicious	Antivirus Detection	Reputation
prisamexico.net	66.199.141.105	true	true		unknown
mail.prisamexico.net	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	7XCBqj5HLqHcRlU.exe, 00000004.00000002.476530485.0000000002A01000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	7XCBqj5HLqHcRlU.exe, 00000004.00000002.476530485.0000000002A01000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.letsencrypt.org0	7XCBqj5HLqHcRlU.exe, 00000004.00000002.474443610.0000000000D1C000.00000004.00000020.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	7XCBqj5HLqHcRlU.exe, 00000004.00000002.476530485.0000000002A01000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false		high
http://www.tiro.com	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://prisamexico.net	7XCBqj5HLqHcRlU.exe, 00000004.00000002.479342187.0000000002CB8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://r3.i.lencr.org/0	7XCBqj5HLqHcRlU.exe, 00000004.00000002.474443610.0000000000D1C000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false		high
http://mail.prisamexico.net	7XCBqj5HLqHcRlU.exe, 00000004.00000002.479342187.0000000002CB8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://yjaeXK8No5PRZuzN.net	7XCBqj5HLqHcRlU.exe, 00000004.00000002.479080463.0000000002C80000.00000004.00000001.sdmp, 7XCBqj5HLqHcRlU.exe, 00000004.00000002.479428427.0000000002CE4000.00000004.00000001.sdmp, 7XCBqj5HLqHcRlU.exe, 00000004.00000002.476530485.0000000002A01000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.o.lencr.org0	7XCBqj5HLqHcRlU.exe, 00000004.00000002.474443610.0000000000D1C000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false		high
http://www.fonts.com	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://hDgEgh.com	7XCBqj5HLqHcRlU.exe, 00000004.00000002.476530485.0000000002A01000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	7XCBqj5HLqHcRlU.exe, 00000000.00000002.246783403.0000000005B30000.00000002.00000001.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	7XCBqj5HLqHcRlU.exe, 00000000.00000002.241704135.0000000003DFF000.00000004.00000001.sdmp, 7XCBqj5HLqHcRlU.exe, 00000004.00000002.471184243.0000000004002000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.root-x1.letsencrypt.org0	7XCBqj5HLqHcRlU.exe, 00000004.00000002.474443610.0000000000D1C000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.199.141.105	prisamexico.net	Canada		13768	COGECO-PEER1CA	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404247
Start date:	04.05.2021
Start time:	20:44:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7XCBqj5HLqHcRlU.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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@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): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 2.20.157.220, 104.42.151.234, 52.255.188.83, 23.57.80.111, 20.82.210.154, 2.20.142.209, 2.20.142.210, 92.122.213.194, 92.122.213.247, 20.54.26.129, 20.49.157.6 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/404247/sample/7XCBqj5HLqHcRlU.exe

Simulations

Behavior and APIs

Time	Type	Description
20:45:59	API Interceptor	715x Sleep call for process: 7XCBqj5HLqHcRlU.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
COGECO-PEER1CA	generated check 662732.xlsm	Get hash	malicious	Browse	• 64.34.68.10
	4JQil8gLKd	Get hash	malicious	Browse	• 185.33.5.160
	Radix_1_exe.exe	Get hash	malicious	Browse	• 209.15.37.6
	Missed +443547900.wav - 45551 PM.htm.htm	Get hash	malicious	Browse	• 76.74.184.111
	#Ud83d#UdcdeMissed +60475998.wav - 82218 PM.htm	Get hash	malicious	Browse	• 76.74.184.111
	#Ud83d#UdcdeMissed +1957636658.wav - 63542 PM.htm .htm	Get hash	malicious	Browse	• 76.74.184.111
	z2xQEFs54b.exe	Get hash	malicious	Browse	• 76.74.184.61
	IMG-03-14-2021.exe	Get hash	malicious	Browse	• 69.90.160.170
	QUOTATION 03112021.exe	Get hash	malicious	Browse	• 69.90.160.170
	QUOTATION 03112021.exe	Get hash	malicious	Browse	• 69.90.160.170
	QUOTATION 03102021.exe	Get hash	malicious	Browse	• 69.90.160.170
	Avis de Paiement (1).xlsx	Get hash	malicious	Browse	• 66.155.71.149
	Agency Appointment - MV Patagonia.doc	Get hash	malicious	Browse	• 69.90.160.10
	remittanceslip_pdf.exe	Get hash	malicious	Browse	• 209.15.37.6
	New_Order.exe	Get hash	malicious	Browse	• 69.90.160.170
	tS9P6wPz9x.exe	Get hash	malicious	Browse	• 66.155.35.240
	ransomware.exe	Get hash	malicious	Browse	• 66.155.35.240
	ransomware.exe	Get hash	malicious	Browse	• 66.155.35.240
	m9vk5iD1xh.exe	Get hash	malicious	Browse	• 69.90.160.170

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\7XCBqj5HLqHcRlU.exe.log

Process:	C:\Users\user\Desktop\7XCBqj5HLqHcRlU.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

Static File Info

General

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.139562078643783
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	7XCBqj5HLqHcRlU.exe
File size:	1027584
MD5:	09a25586d2eaf5e8c3a5df5557bad218
SHA1:	33acc64a84386fc9b14c9b389f7fc7f4fad089e6
SHA256:	e34725603d4f0177a6fbb66cff9f073a90cd74e6a65c05f1a704ab390906474f
SHA512:	f47e7aad5ec8bab9da67d38bc2c41af84a7ee2ae25ae8d65b1430d0c516afbead11828113986250c48a1d71e6e05a19aca914075443236c565232c3cde361670
SSDEEP:	12288:WTbB4fWXY3Ot6InK1sLuNp+dM0kKg0D75wAPG+zETi/Pih2CV5R2DMa46ZSLmFbD:WI6ZS8toLAOAYKOVGNkulYP0tl
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....B.... ....@.. .... @.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4fc142
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:	0xF520A8BD [Wed Apr 28 01:17:49 2100 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

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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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	0xfc0f0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xfe000	0x604	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x100000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xfc0d4	0x1c	.text
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	0xfa148	0xfa200	False	0.619281179723	data	7.14608942237	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xfe000	0x604	0x800	False	0.33154296875	data	3.44527479652	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x100000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xfe090	0x374	data		
RT_MANIFEST	0xfe414	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

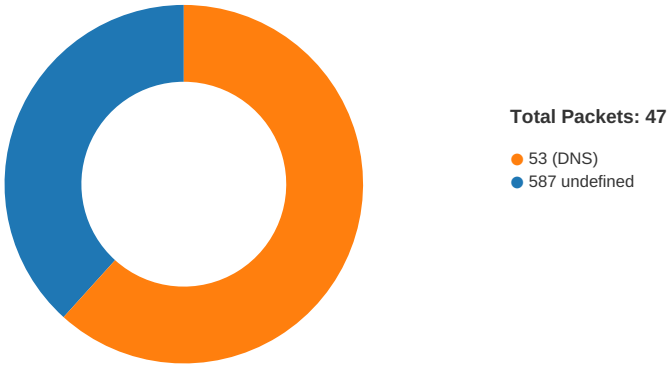
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2019
Assembly Version	1.0.0.0
InternalName	TCUtRTle7N3X8OP.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	HospitalManagementSystem
ProductVersion	1.0.0.0
FileDescription	HospitalManagementSystem
OriginalFilename	TCUtRTle7N3X8OP.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:47:40.708321095 CEST	49737	587	192.168.2.3	66.199.141.105
May 4, 2021 20:47:40.843053102 CEST	587	49737	66.199.141.105	192.168.2.3
May 4, 2021 20:47:40.843238115 CEST	49737	587	192.168.2.3	66.199.141.105
May 4, 2021 20:47:41.093657017 CEST	587	49737	66.199.141.105	192.168.2.3
May 4, 2021 20:47:41.093995094 CEST	49737	587	192.168.2.3	66.199.141.105
May 4, 2021 20:47:41.229269028 CEST	587	49737	66.199.141.105	192.168.2.3
May 4, 2021 20:47:41.229557991 CEST	49737	587	192.168.2.3	66.199.141.105
May 4, 2021 20:47:41.365915060 CEST	587	49737	66.199.141.105	192.168.2.3
May 4, 2021 20:47:41.400036097 CEST	49737	587	192.168.2.3	66.199.141.105
May 4, 2021 20:47:41.547707081 CEST	587	49737	66.199.141.105	192.168.2.3
May 4, 2021 20:47:41.547727108 CEST	587	49737	66.199.141.105	192.168.2.3
May 4, 2021 20:47:41.547743082 CEST	587	49737	66.199.141.105	192.168.2.3
May 4, 2021 20:47:41.547852993 CEST	49737	587	192.168.2.3	66.199.141.105
May 4, 2021 20:47:41.555566072 CEST	49737	587	192.168.2.3	66.199.141.105
May 4, 2021 20:47:41.690119028 CEST	587	49737	66.199.141.105	192.168.2.3
May 4, 2021 20:47:41.737818956 CEST	49737	587	192.168.2.3	66.199.141.105
May 4, 2021 20:47:41.872133970 CEST	587	49737	66.199.141.105	192.168.2.3
May 4, 2021 20:47:41.874854088 CEST	49737	587	192.168.2.3	66.199.141.105
May 4, 2021 20:47:42.009603977 CEST	587	49737	66.199.141.105	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:47:42.010371923 CEST	49737	587	192.168.2.3	66.199.141.105
May 4, 2021 20:47:42.145611048 CEST	587	49737	66.199.141.105	192.168.2.3
May 4, 2021 20:47:42.146420956 CEST	49737	587	192.168.2.3	66.199.141.105
May 4, 2021 20:47:42.282630920 CEST	587	49737	66.199.141.105	192.168.2.3
May 4, 2021 20:47:42.283515930 CEST	49737	587	192.168.2.3	66.199.141.105
May 4, 2021 20:47:42.419806004 CEST	587	49737	66.199.141.105	192.168.2.3
May 4, 2021 20:47:42.420697927 CEST	49737	587	192.168.2.3	66.199.141.105
May 4, 2021 20:47:42.557286024 CEST	587	49737	66.199.141.105	192.168.2.3
May 4, 2021 20:47:42.563513994 CEST	49737	587	192.168.2.3	66.199.141.105
May 4, 2021 20:47:42.563889027 CEST	49737	587	192.168.2.3	66.199.141.105
May 4, 2021 20:47:42.564095974 CEST	49737	587	192.168.2.3	66.199.141.105
May 4, 2021 20:47:42.564300060 CEST	49737	587	192.168.2.3	66.199.141.105
May 4, 2021 20:47:42.698018074 CEST	587	49737	66.199.141.105	192.168.2.3
May 4, 2021 20:47:42.698143005 CEST	587	49737	66.199.141.105	192.168.2.3
May 4, 2021 20:47:42.698236942 CEST	587	49737	66.199.141.105	192.168.2.3
May 4, 2021 20:47:42.698370934 CEST	587	49737	66.199.141.105	192.168.2.3
May 4, 2021 20:47:43.438055992 CEST	587	49737	66.199.141.105	192.168.2.3
May 4, 2021 20:47:43.491334915 CEST	49737	587	192.168.2.3	66.199.141.105

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:45:40.907846928 CEST	49199	53	192.168.2.3	8.8.8.8
May 4, 2021 20:45:40.958323956 CEST	53	49199	8.8.8.8	192.168.2.3
May 4, 2021 20:45:41.885293007 CEST	50620	53	192.168.2.3	8.8.8.8
May 4, 2021 20:45:41.944705963 CEST	53	50620	8.8.8.8	192.168.2.3
May 4, 2021 20:45:42.101284981 CEST	64938	53	192.168.2.3	8.8.8.8
May 4, 2021 20:45:42.152767897 CEST	53	64938	8.8.8.8	192.168.2.3
May 4, 2021 20:45:43.249723911 CEST	60152	53	192.168.2.3	8.8.8.8
May 4, 2021 20:45:43.300298929 CEST	53	60152	8.8.8.8	192.168.2.3
May 4, 2021 20:45:44.250201941 CEST	57544	53	192.168.2.3	8.8.8.8
May 4, 2021 20:45:44.299710035 CEST	53	57544	8.8.8.8	192.168.2.3
May 4, 2021 20:45:45.148391008 CEST	55984	53	192.168.2.3	8.8.8.8
May 4, 2021 20:45:45.199253082 CEST	53	55984	8.8.8.8	192.168.2.3
May 4, 2021 20:45:46.306448936 CEST	64185	53	192.168.2.3	8.8.8.8
May 4, 2021 20:45:46.357938051 CEST	53	64185	8.8.8.8	192.168.2.3
May 4, 2021 20:45:47.115859032 CEST	65110	53	192.168.2.3	8.8.8.8
May 4, 2021 20:45:47.173021078 CEST	53	65110	8.8.8.8	192.168.2.3
May 4, 2021 20:45:48.256779909 CEST	58361	53	192.168.2.3	8.8.8.8
May 4, 2021 20:45:48.318157911 CEST	53	58361	8.8.8.8	192.168.2.3
May 4, 2021 20:45:49.302977085 CEST	63492	53	192.168.2.3	8.8.8.8
May 4, 2021 20:45:49.354597092 CEST	53	63492	8.8.8.8	192.168.2.3
May 4, 2021 20:45:50.800856113 CEST	60831	53	192.168.2.3	8.8.8.8
May 4, 2021 20:45:50.849457979 CEST	53	60831	8.8.8.8	192.168.2.3
May 4, 2021 20:45:51.602194071 CEST	60100	53	192.168.2.3	8.8.8.8
May 4, 2021 20:45:51.653870106 CEST	53	60100	8.8.8.8	192.168.2.3
May 4, 2021 20:45:52.488270998 CEST	53195	53	192.168.2.3	8.8.8.8
May 4, 2021 20:45:52.537082911 CEST	53	53195	8.8.8.8	192.168.2.3
May 4, 2021 20:45:53.319747925 CEST	50141	53	192.168.2.3	8.8.8.8
May 4, 2021 20:45:53.371381998 CEST	53	50141	8.8.8.8	192.168.2.3
May 4, 2021 20:45:54.418693066 CEST	53023	53	192.168.2.3	8.8.8.8
May 4, 2021 20:45:54.469448090 CEST	53	53023	8.8.8.8	192.168.2.3
May 4, 2021 20:45:55.268682003 CEST	49563	53	192.168.2.3	8.8.8.8
May 4, 2021 20:45:55.321857929 CEST	53	49563	8.8.8.8	192.168.2.3
May 4, 2021 20:45:56.490590096 CEST	51352	53	192.168.2.3	8.8.8.8
May 4, 2021 20:45:56.550529003 CEST	53	51352	8.8.8.8	192.168.2.3
May 4, 2021 20:45:57.402920008 CEST	59349	53	192.168.2.3	8.8.8.8
May 4, 2021 20:45:57.460558891 CEST	53	59349	8.8.8.8	192.168.2.3
May 4, 2021 20:46:15.903362036 CEST	57084	53	192.168.2.3	8.8.8.8
May 4, 2021 20:46:15.963665009 CEST	53	57084	8.8.8.8	192.168.2.3
May 4, 2021 20:46:19.540618896 CEST	58823	53	192.168.2.3	8.8.8.8
May 4, 2021 20:46:19.589715958 CEST	53	58823	8.8.8.8	192.168.2.3
May 4, 2021 20:46:35.394798040 CEST	57568	53	192.168.2.3	8.8.8.8
May 4, 2021 20:46:35.454495907 CEST	53	57568	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:46:40.774811029 CEST	50540	53	192.168.2.3	8.8.8.8
May 4, 2021 20:46:40.840569973 CEST	53	50540	8.8.8.8	192.168.2.3
May 4, 2021 20:46:52.624903917 CEST	54366	53	192.168.2.3	8.8.8.8
May 4, 2021 20:46:52.681967020 CEST	53	54366	8.8.8.8	192.168.2.3
May 4, 2021 20:47:02.382545948 CEST	53034	53	192.168.2.3	8.8.8.8
May 4, 2021 20:47:02.454353094 CEST	53	53034	8.8.8.8	192.168.2.3
May 4, 2021 20:47:06.082418919 CEST	57762	53	192.168.2.3	8.8.8.8
May 4, 2021 20:47:06.147727013 CEST	53	57762	8.8.8.8	192.168.2.3
May 4, 2021 20:47:37.567984104 CEST	55435	53	192.168.2.3	8.8.8.8
May 4, 2021 20:47:37.633315086 CEST	53	55435	8.8.8.8	192.168.2.3
May 4, 2021 20:47:40.341852903 CEST	50713	53	192.168.2.3	8.8.8.8
May 4, 2021 20:47:40.495930910 CEST	53	50713	8.8.8.8	192.168.2.3
May 4, 2021 20:47:40.520329952 CEST	56132	53	192.168.2.3	8.8.8.8
May 4, 2021 20:47:40.596545935 CEST	58987	53	192.168.2.3	8.8.8.8
May 4, 2021 20:47:40.669444084 CEST	53	58987	8.8.8.8	192.168.2.3
May 4, 2021 20:47:40.685180902 CEST	53	56132	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 20:47:40.341852903 CEST	192.168.2.3	8.8.8.8	0x1ba7	Standard query (0)	mail.prisa mexico.net	A (IP address)	IN (0x0001)
May 4, 2021 20:47:40.520329952 CEST	192.168.2.3	8.8.8.8	0xde31	Standard query (0)	mail.prisa mexico.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:47:40.495930910 CEST	8.8.8.8	192.168.2.3	0x1ba7	No error (0)	mail.prisa mexico.net	prisamexico.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:47:40.495930910 CEST	8.8.8.8	192.168.2.3	0x1ba7	No error (0)	prisamexico.net		66.199.141.105	A (IP address)	IN (0x0001)
May 4, 2021 20:47:40.685180902 CEST	8.8.8.8	192.168.2.3	0xde31	No error (0)	mail.prisa mexico.net	prisamexico.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:47:40.685180902 CEST	8.8.8.8	192.168.2.3	0xde31	No error (0)	prisamexico.net		66.199.141.105	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 4, 2021 20:47:41.093657017 CEST	587	49737	66.199.141.105	192.168.2.3	220-r130.websiteservername.com ESMTP Exim 4.94.2 #2 Tue, 04 May 2021 13:47:41 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 4, 2021 20:47:41.093995094 CEST	49737	587	192.168.2.3	66.199.141.105	EHLO 888683
May 4, 2021 20:47:41.229269028 CEST	587	49737	66.199.141.105	192.168.2.3	250-r130.websiteservername.com Hello 888683 [84.17.52.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 4, 2021 20:47:41.229557991 CEST	49737	587	192.168.2.3	66.199.141.105	STARTTLS
May 4, 2021 20:47:41.365915060 CEST	587	49737	66.199.141.105	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 7XCBqj5HLqHcRlU.exe PID: 5452 Parent PID: 5764

General

Start time:	20:45:48
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\7XCBqj5HLqHcRlU.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\7XCBqj5HLqHcRlU.exe'
Imagebase:	0x730000
File size:	1027584 bytes
MD5 hash:	09A25586D2EAF5E8C3A5DF5557BAD218
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: 00000000.00000002.241704135.0000000003DFF000.00000004.00000001.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	6DEBCF06	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	6DEBCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\7XCBqj5HLqHcRlU.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1CC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\7XCBqj5HLqHcRlU.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 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	6E1CC907	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	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile

Analysis Process: 7XCBqj5HLqHcRlU.exe PID: 5628 Parent PID: 5452

General

Start time:	20:46:00
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\7XCBqj5HLqHcRlU.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x510000
File size:	1027584 bytes
MD5 hash:	09A25586D2EAF5E8C3A5DF5557BAD218

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: 00000004.00000002.471184243.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.476530485.0000000002A01000.00000004.00000001.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	6DEBCF06	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	6DEBCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\4ff67223-8361-494b-bb32-721ca0f2bd8a	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6CD01B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CD01B4F	ReadFile

Disassembly

Code Analysis