ID: 404232
Sample Name: Drawing & Specification.exe
Cookbook: default.jbs
Time: 20:27:21
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

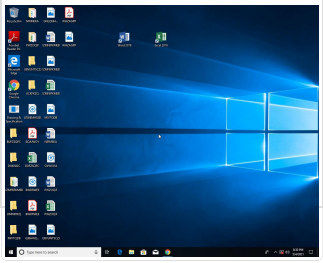
Analysis Report Drawing & Specification.exe

Overview

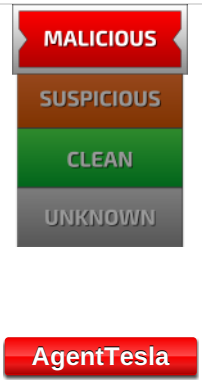
General Information

Sample Name:	Drawing & Specification.exe
Analysis ID:	404232
MD5:	ca335d0db05f4d6.
SHA1:	25fe5dee878bd82.
SHA256:	27bb1e8bbd36d0..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

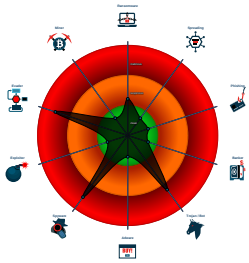


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected AgentTesla
- Yara detected AntiVM3
- 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…
- Tries to harvest and steal ftp login c…
- Tries to steal Mail credentials (via fil…

Classification



Startup

- **System is w10x64**
- Drawing & Specification.exe (PID: 7024 cmdline: 'C:\Users\user\Desktop\Drawing & Specification.exe' MD5: CA335D0DB05F4D6FB2063FAFE1A72959)
  - RegSvcs.exe (PID: 2912 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "lnfo@buzon-th.comEawrAmEfowmail.buzon-th.comworksuccessful@yandex.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.912250246.00000000029C1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.912250246.00000000029C1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000002.00000002.911036255.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.669225825.0000000004029000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: RegSvcs.exe PID: 2912	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 3 entries

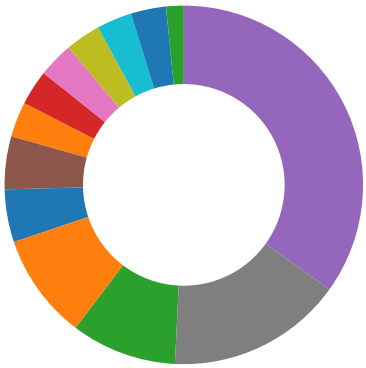
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Drawing & Specification.exe.42a0240.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Drawing & Specification.exe.42a0240.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Drawing & Specification.exe.41fd820.2.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:

Found malware configuration

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

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)

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)

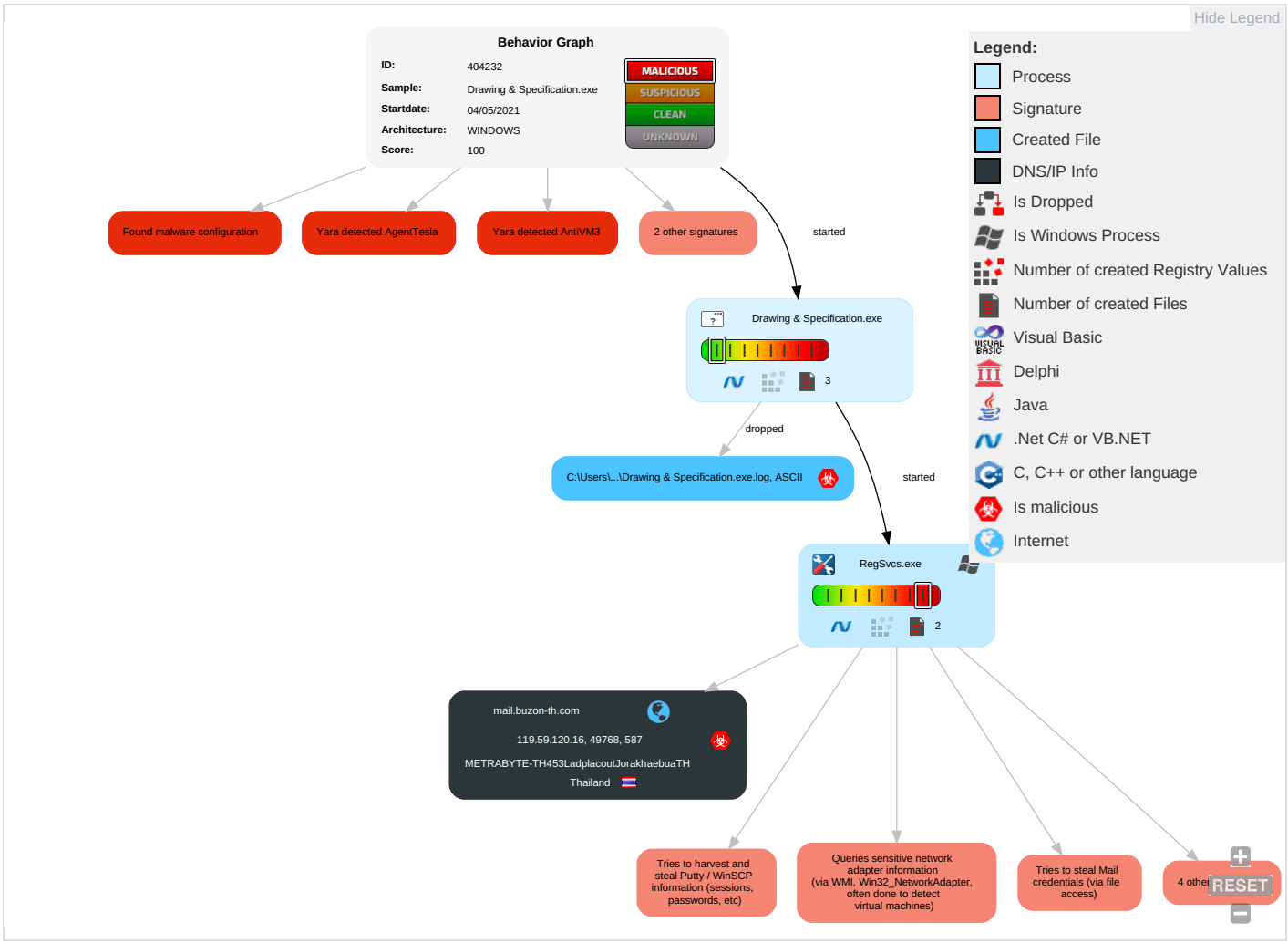
Remote Access Functionality:

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	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 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	Obfuscated Files or Information 2	Input Capture 1 1	Query Registry 1	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 2	Credentials in Registry 1	Security Software Discovery 2 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Timestomp 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

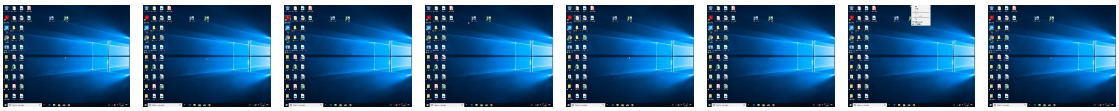
Behavior Graph



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
Drawing & Specification.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.RegSvcs.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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://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.goodfont.co.kr	0%	URL Reputation	safe	
http://https://x2g5XHAct4sZc8i.com	0%	Avira URL Cloud	safe	
http://ZRbCEB.com	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://www.carterandcone.coml	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.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.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.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://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://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://mail.buzon-th.com	0%	Avira URL Cloud	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://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.buzon-th.com	119.59.120.16	true	true		unknown

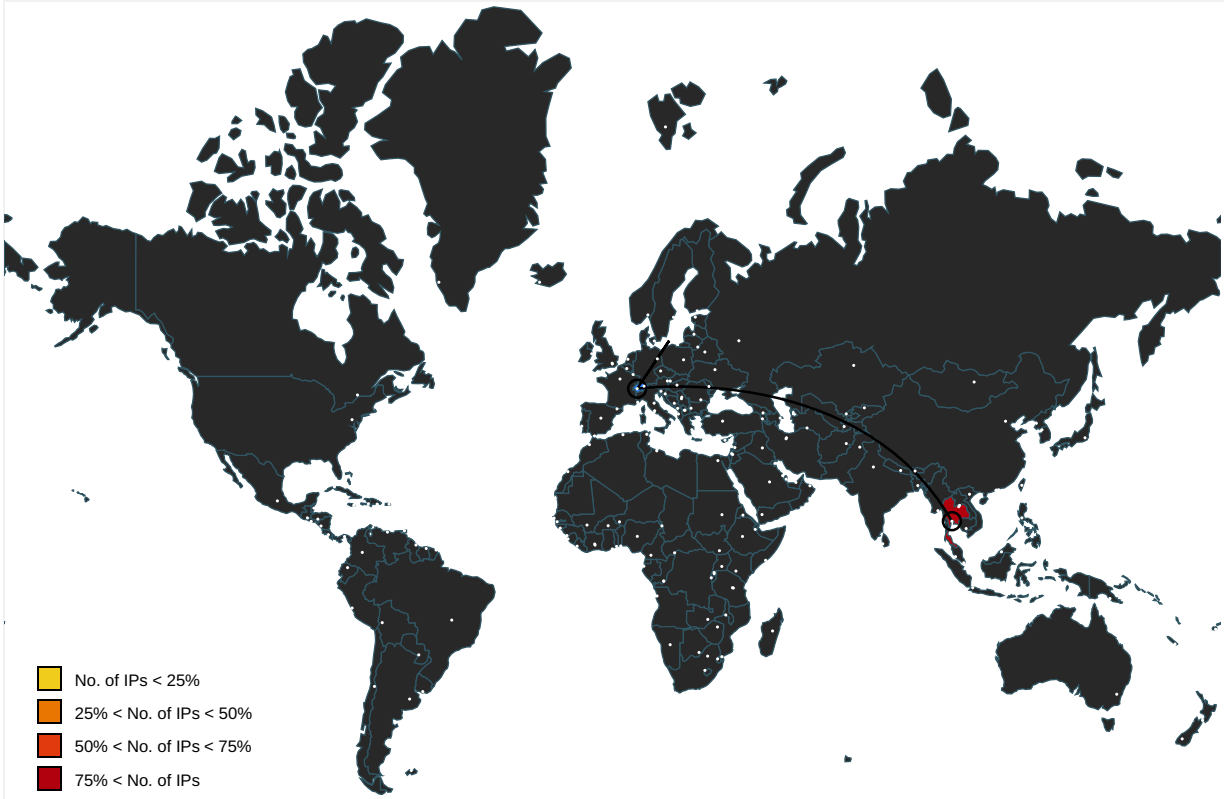
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegSvcs.exe, 00000002.00000002.912250246.00000000029C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	RegSvcs.exe, 00000002.00000002.912250246.00000000029C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegSvcs.exe, 00000002.00000002.912250246.00000000029C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false		high
http://www.tiro.com	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://x2g5XHAct4sZc8i.com	RegSvcs.exe, 00000002.00000002.912250246.00000000029C1000.00000004.00000001.sdmp, RegSvcs.exe, 00000002.00000002.912682451.0000000002D15000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ZRbCEB.com	RegSvcs.exe, 00000002.00000002.912250246.00000000029C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.buzon-th.com	RegSvcs.exe, 00000002.00000002.912697562.0000000002D1D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false		high
http://www.fonts.com	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	Drawing & Specification.exe, 00000000.00000002.672830284.0000006070000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Drawing & Specification.exe, 00000000.00000002.669225825.00000000004029000.00000004.00000001.sdmp, RegSvcs.exe, 00000002.00000002.911036255.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
119.59.120.16	mail.buzon-th.com	Thailand		56067	METRABYTE-TH453LadplacoutJorakhaebuaTH	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404232
Start date:	04.05.2021
Start time:	20:27:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Drawing & Specification.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:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
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 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 52.255.188.83, 13.88.21.125, 104.43.139.144, 104.42.151.234, 52.147.198.201, 20.82.210.154, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus16.cloudapp.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, skypedataprdcoleus16.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, blobcollector.events.data.trafficmanager.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:28:18	API Interceptor	1x Sleep call for process: Drawing & Specification.exe modified
20:28:28	API Interceptor	763x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
119.59.120.16	Commercial Imports Inquiry - Import.exe	Get hash	malicious	Browse	
	PO 9506.exe	Get hash	malicious	Browse	
	PO 9506.exe	Get hash	malicious	Browse	
	RFQCSDOK202140890.exe	Get hash	malicious	Browse	
	Invitation for Tender RFQCSDOK202140890.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
METRABYTE-TH453LadplacoutJorakhaebuaTH	Commercial Imports Inquiry - Import.exe	Get hash	malicious	Browse	• 119.59.120.16
	v8iFmF7XPp.dll	Get hash	malicious	Browse	• 119.59.116.21
	PO 9506.exe	Get hash	malicious	Browse	• 119.59.120.16
	PO 9506.exe	Get hash	malicious	Browse	• 119.59.120.16
	RFQCSDOK202140890.exe	Get hash	malicious	Browse	• 119.59.120.16
	Invitation for Tender RFQCSDOK202140890.exe	Get hash	malicious	Browse	• 119.59.120.16
	lK8vF3n2e7.exe	Get hash	malicious	Browse	• 119.59.124.163
	ZGNbR8E726.exe	Get hash	malicious	Browse	• 119.59.120.8
	PO032321.exe	Get hash	malicious	Browse	• 119.59.96.105
	payment proof.xlsx	Get hash	malicious	Browse	• 119.59.120.8
	2ojdmC51As.exe	Get hash	malicious	Browse	• 119.59.116.21
	NEW PURCHASE030421.exe	Get hash	malicious	Browse	• 119.59.96.105
	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	• 119.59.116.21
	HUNL5V-011220.doc	Get hash	malicious	Browse	• 119.59.116.174
	RFQ-1225 BE285-20-B-1-SMcS - Easi-Clip Project.exe	Get hash	malicious	Browse	• 119.59.120.8
	IKT7vWaI2V.exe	Get hash	malicious	Browse	• 119.59.120.8
	KP5ESTzrF8.exe	Get hash	malicious	Browse	• 119.59.120.8
	http://https://dusitserve.com/gethits/o3A/	Get hash	malicious	Browse	• 119.59.125.211
	http://danngoschool.net/modules/infodata.php?r=bD1odHRwczovL3VzcHNzZXJ2aWNlcy5zZWNseXNldGV0dXIudGs=	Get hash	malicious	Browse	• 119.59.125.245

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Drawing & Specification.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

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

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.175356450068055
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:	Drawing & Specification.exe
File size:	1056768
MD5:	ca335d0db05f4d6fb2063fafe1a72959
SHA1:	25fe5dee878bd82f02992e82f1af815dc5c64aef
SHA256:	27bb1e8bbd36d0bdb7e746bcc349ed5e440f1fd471503b6ae6754c9d95b069d9
SHA512:	5661d447137710ab8c5aa3170e55b2ead6141e3d9fc1584197dc385b165e261007f6c20bd86df8cbdd13ecc8562c44423ab01ce5426abe5198da0f599a0da398
SSDEEP:	24576:pD9wLdzoLA+YorlMJLp73Swf3zd+64J7/xV:pD9wLdOYMlq3Swfh+7ZV
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...qH@.....0.....2... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x5032d6
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:	0xDD404871 [Sun Aug 17 16:53:05 2087 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x103284	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x104000	0x604	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x106000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x103268	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	0x1012dc	0x101400	False	0.629728118926	COM executable for DOS	7.18172287887	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x104000	0x604	0x800	False	0.32861328125	data	3.43664593961	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x106000	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	0x104090	0x374	data		
RT_MANIFEST	0x104414	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

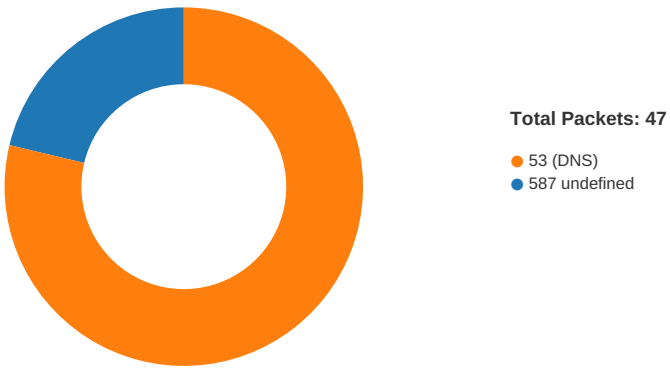
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2019
Assembly Version	1.0.0.0
InternalName	T5P81mHIq4ryrUR.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	HospitalManagementSystem
ProductVersion	1.0.0.0
FileDescription	HospitalManagementSystem
OriginalFilename	T5P81mHIq4ryrUR.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:29:53.508924961 CEST	49768	587	192.168.2.4	119.59.120.16
May 4, 2021 20:29:53.759125948 CEST	587	49768	119.59.120.16	192.168.2.4
May 4, 2021 20:29:53.759469986 CEST	49768	587	192.168.2.4	119.59.120.16
May 4, 2021 20:29:54.568589926 CEST	587	49768	119.59.120.16	192.168.2.4
May 4, 2021 20:29:54.569161892 CEST	49768	587	192.168.2.4	119.59.120.16

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:29:54.823471069 CEST	587	49768	119.59.120.16	192.168.2.4
May 4, 2021 20:29:54.825124979 CEST	49768	587	192.168.2.4	119.59.120.16
May 4, 2021 20:29:55.075512886 CEST	587	49768	119.59.120.16	192.168.2.4
May 4, 2021 20:29:55.076440096 CEST	49768	587	192.168.2.4	119.59.120.16
May 4, 2021 20:29:55.333353996 CEST	587	49768	119.59.120.16	192.168.2.4
May 4, 2021 20:29:55.334532976 CEST	49768	587	192.168.2.4	119.59.120.16
May 4, 2021 20:29:55.586198092 CEST	587	49768	119.59.120.16	192.168.2.4
May 4, 2021 20:29:55.586853981 CEST	49768	587	192.168.2.4	119.59.120.16
May 4, 2021 20:29:55.837502003 CEST	587	49768	119.59.120.16	192.168.2.4
May 4, 2021 20:29:55.844007969 CEST	49768	587	192.168.2.4	119.59.120.16
May 4, 2021 20:29:56.094223976 CEST	587	49768	119.59.120.16	192.168.2.4
May 4, 2021 20:29:56.094351053 CEST	49768	587	192.168.2.4	119.59.120.16
May 4, 2021 20:29:56.094496012 CEST	587	49768	119.59.120.16	192.168.2.4
May 4, 2021 20:29:56.094559908 CEST	49768	587	192.168.2.4	119.59.120.16

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:28:01.598270893 CEST	53	53097	8.8.8.8	192.168.2.4
May 4, 2021 20:28:02.147885084 CEST	49257	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:02.197666883 CEST	53	49257	8.8.8.8	192.168.2.4
May 4, 2021 20:28:02.963413000 CEST	62389	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:03.012417078 CEST	53	62389	8.8.8.8	192.168.2.4
May 4, 2021 20:28:04.062186956 CEST	49910	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:04.113573074 CEST	53	49910	8.8.8.8	192.168.2.4
May 4, 2021 20:28:04.966531038 CEST	55854	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:05.020010948 CEST	53	55854	8.8.8.8	192.168.2.4
May 4, 2021 20:28:05.989820957 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:06.038608074 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 20:28:07.383656025 CEST	63153	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:07.442735910 CEST	53	63153	8.8.8.8	192.168.2.4
May 4, 2021 20:28:08.389559984 CEST	52991	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:08.441006899 CEST	53	52991	8.8.8.8	192.168.2.4
May 4, 2021 20:28:09.380465031 CEST	53700	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:09.431746960 CEST	53	53700	8.8.8.8	192.168.2.4
May 4, 2021 20:28:10.683351040 CEST	51726	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:10.737530947 CEST	53	51726	8.8.8.8	192.168.2.4
May 4, 2021 20:28:11.582832098 CEST	56794	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:11.631705999 CEST	53	56794	8.8.8.8	192.168.2.4
May 4, 2021 20:28:12.568325996 CEST	56534	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:12.618863106 CEST	53	56534	8.8.8.8	192.168.2.4
May 4, 2021 20:28:13.769159079 CEST	56627	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:13.822519064 CEST	53	56627	8.8.8.8	192.168.2.4
May 4, 2021 20:28:14.687386990 CEST	56621	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:14.738053083 CEST	53	56621	8.8.8.8	192.168.2.4
May 4, 2021 20:28:15.591723919 CEST	63116	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:15.642194986 CEST	53	63116	8.8.8.8	192.168.2.4
May 4, 2021 20:28:16.614829063 CEST	64078	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:16.664134026 CEST	53	64078	8.8.8.8	192.168.2.4
May 4, 2021 20:28:17.855475903 CEST	64801	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:17.904206991 CEST	53	64801	8.8.8.8	192.168.2.4
May 4, 2021 20:28:19.454796076 CEST	61721	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:19.503822088 CEST	53	61721	8.8.8.8	192.168.2.4
May 4, 2021 20:28:20.652977943 CEST	51255	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:20.704464912 CEST	53	51255	8.8.8.8	192.168.2.4
May 4, 2021 20:28:21.597219944 CEST	61522	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:21.648787975 CEST	53	61522	8.8.8.8	192.168.2.4
May 4, 2021 20:28:32.161971092 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:32.211967945 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 20:28:48.574110985 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:48.706023932 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 20:28:49.444298983 CEST	49612	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:49.573468924 CEST	53	49612	8.8.8.8	192.168.2.4
May 4, 2021 20:28:50.188287973 CEST	49285	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:28:50.365406036 CEST	53	49285	8.8.8.8	192.168.2.4
May 4, 2021 20:28:50.632070065 CEST	50601	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:50.709268093 CEST	53	50601	8.8.8.8	192.168.2.4
May 4, 2021 20:28:50.813178062 CEST	60875	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:50.872947931 CEST	53	60875	8.8.8.8	192.168.2.4
May 4, 2021 20:28:51.383491039 CEST	56448	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:51.440538883 CEST	53	56448	8.8.8.8	192.168.2.4
May 4, 2021 20:28:51.972681999 CEST	59172	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:52.029571056 CEST	53	59172	8.8.8.8	192.168.2.4
May 4, 2021 20:28:52.518791914 CEST	62420	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:52.580912113 CEST	53	62420	8.8.8.8	192.168.2.4
May 4, 2021 20:28:53.303570032 CEST	60579	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:53.361498117 CEST	53	60579	8.8.8.8	192.168.2.4
May 4, 2021 20:28:54.176440954 CEST	50183	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:54.238246918 CEST	53	50183	8.8.8.8	192.168.2.4
May 4, 2021 20:28:54.902534962 CEST	61531	53	192.168.2.4	8.8.8.8
May 4, 2021 20:28:54.951093912 CEST	53	61531	8.8.8.8	192.168.2.4
May 4, 2021 20:29:08.011720896 CEST	49228	53	192.168.2.4	8.8.8.8
May 4, 2021 20:29:08.085035086 CEST	53	49228	8.8.8.8	192.168.2.4
May 4, 2021 20:29:08.208712101 CEST	59794	53	192.168.2.4	8.8.8.8
May 4, 2021 20:29:08.274512053 CEST	53	59794	8.8.8.8	192.168.2.4
May 4, 2021 20:29:13.951487064 CEST	55916	53	192.168.2.4	8.8.8.8
May 4, 2021 20:29:14.020479918 CEST	53	55916	8.8.8.8	192.168.2.4
May 4, 2021 20:29:46.758183956 CEST	52752	53	192.168.2.4	8.8.8.8
May 4, 2021 20:29:46.817074060 CEST	53	52752	8.8.8.8	192.168.2.4
May 4, 2021 20:29:48.581024885 CEST	60542	53	192.168.2.4	8.8.8.8
May 4, 2021 20:29:48.641463995 CEST	53	60542	8.8.8.8	192.168.2.4
May 4, 2021 20:29:53.091742039 CEST	60689	53	192.168.2.4	8.8.8.8
May 4, 2021 20:29:53.487273932 CEST	53	60689	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 20:29:53.091742039 CEST	192.168.2.4	8.8.8.8	0xabe7	Standard query (0)	mail.buzon-th.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:29:53.487273932 CEST	8.8.8.8	192.168.2.4	0xabe7	No error (0)	mail.buzon-th.com		119.59.120.16	A (IP address)	IN (0x0001)

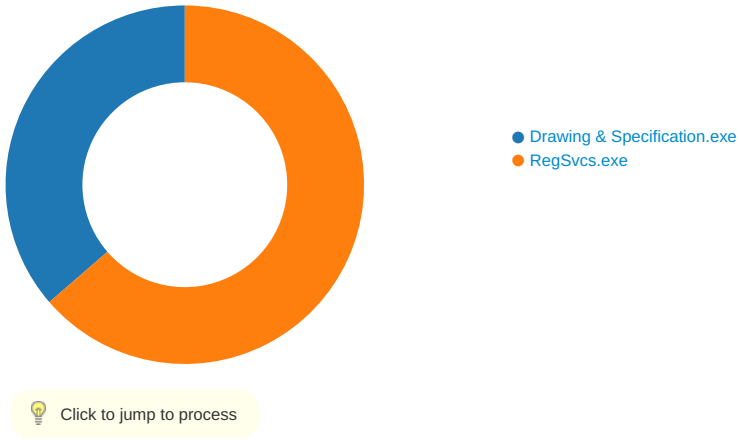
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 4, 2021 20:29:54.568589926 CEST	587	49768	119.59.120.16	192.168.2.4	220 ns97.hostinglotus.net ESMTP Exim 4.92.3 Wed, 05 May 2021 01:29:54 +0700
May 4, 2021 20:29:54.569161892 CEST	49768	587	192.168.2.4	119.59.120.16	EHLO 472847
May 4, 2021 20:29:54.823471069 CEST	587	49768	119.59.120.16	192.168.2.4	250-ns97.hostinglotus.net Hello 472847 [84.17.52.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 4, 2021 20:29:54.825124979 CEST	49768	587	192.168.2.4	119.59.120.16	AUTH login bG5mb0BidXpvbi10aC5jb20=
May 4, 2021 20:29:55.075512886 CEST	587	49768	119.59.120.16	192.168.2.4	334 UGFzc3dvcmQ6
May 4, 2021 20:29:55.333353996 CEST	587	49768	119.59.120.16	192.168.2.4	535 Incorrect authentication data
May 4, 2021 20:29:55.334532976 CEST	49768	587	192.168.2.4	119.59.120.16	MAIL FROM:<lnfo@buzon-th.com>
May 4, 2021 20:29:55.586198092 CEST	587	49768	119.59.120.16	192.168.2.4	250 OK
May 4, 2021 20:29:55.586853981 CEST	49768	587	192.168.2.4	119.59.120.16	RCPT TO:<worksuccessful@yandex.com>
May 4, 2021 20:29:55.837502003 CEST	587	49768	119.59.120.16	192.168.2.4	550 relay not permitted, authentication required
May 4, 2021 20:29:56.094223976 CEST	587	49768	119.59.120.16	192.168.2.4	421 ns97.hostinglotus.net lost input connection

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Drawing & Specification.exe PID: 7024 Parent PID: 5976

General

Start time:	20:28:09
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\Drawing & Specification.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Drawing & Specification.exe'
Imagebase:	0xbd0000
File size:	1056768 bytes
MD5 hash:	CA335D0DB05F4D6FB2063FAFE1A72959
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: 00000000.00000002.669225825.0000000004029000.00000004.00000001.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	6D20CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D20CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Drawing & Specification.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D51C78D	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\Drawing & Specification.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	6D51C907	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	6D1E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C051B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C051B4F	ReadFile

Analysis Process: RegSvcs.exe PID: 2912 Parent PID: 7024

General

Start time:	20:28:19
Start date:	04/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x540000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000002.00000002.912250246.00000000029C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.912250246.00000000029C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.911036255.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

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	6D20CF06	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	6D20CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D1E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D1E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D1ECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D1ECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C051B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C051B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6C051B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6C051B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D1E5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D1E5705	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C051B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6C051B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\b869cfb1-1df3-4242-acf6-5b73b15ea102	unknown	4096	success or wait	1	6C051B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6C051B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C051B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C051B4F	ReadFile

Disassembly

Code Analysis