ID: 626099
Sample Name: SOA.exe
Cookbook: default.jbs
Time: 15:42:10
Date: 13/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

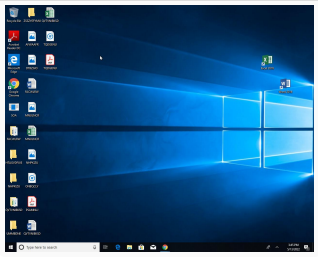
Windows Analysis Report

SOA.exe

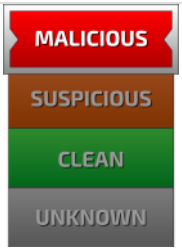
Overview

General Information

Sample Name:	SOA.exe
Analysis ID:	626099
MD5:	f18604d5fc3e293..
SHA1:	aa0517c10c333f...
SHA256:	46584937f3c753..
Tags:	AgentTesla exe
Infos:	



Detection



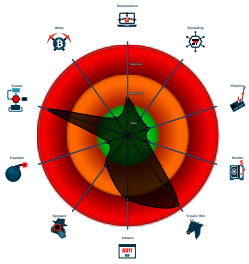
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Yara detected AntiVM3
- Writes to foreign memory regions
- Modifies the hosts file
- Tries to detect sandboxes and other...
- Uses the Telegram API (likely for C...
- Machine Learning detection for sam...
- Injects a PE file into a foreign proce...

Classification



Process Tree

- **System is w10x64**
- SOA.exe (PID: 6968 cmdline: "C:\Users\user\Desktop\SOA.exe" MD5: F18604D5FC3E2930E85C403E0E80A459)
  - RegSvcs.exe (PID: 6360 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot2134979594:AAFk4QkrlHlt2a-q-EhIoHZBbzxSH0QxiBI/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "1295185895",
  "Chat URL": "https://api.telegram.org/bot2134979594:AAFk4QkrlHlt2a-q-EhIoHZBbzxSH0QxiBI/sendDocument"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.700193844.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.700193844.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000006.00000000.474512000.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000000.474512000.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000006.00000000.474083361.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
6.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
6.2.RegSvcs.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30dcf:$s1: get_kbok • 0x3172a:$s2: get_CHoo • 0x3239d:$s3: set_passwordIsSet • 0x30bd3:$s4: get_enableLog • 0x35378:$s8: torbrowser • 0x33d54:$s10: logins • 0x33629:$s11: credential • 0x2ffb6:$g1: get_Clipboard • 0x2ffc4:$g2: get_Keyboard • 0x2ffd1:$g3: get_Password • 0x315d8:$g4: get_CtrlKeyDown • 0x315e8:$g5: get_ShiftKeyDown • 0x315f9:$g6: get_AltKeyDown
6.0.RegSvcs.exe.400000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 30 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Uses the Telegram API (likely for C&C communication)

Yara detected Generic Downloader

Spam, unwanted Advertisements and Ransom Demands

Modifies the hosts file

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Malware Analysis System Evasion

Yara detected AntiVM3

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

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Modifies the hosts file

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings

Modifies the hosts file

Stealing of Sensitive Information

Yara detected Telegram RAT

Yara detected AgentTesla

Remote Access Functionality

Yara detected Telegram RAT

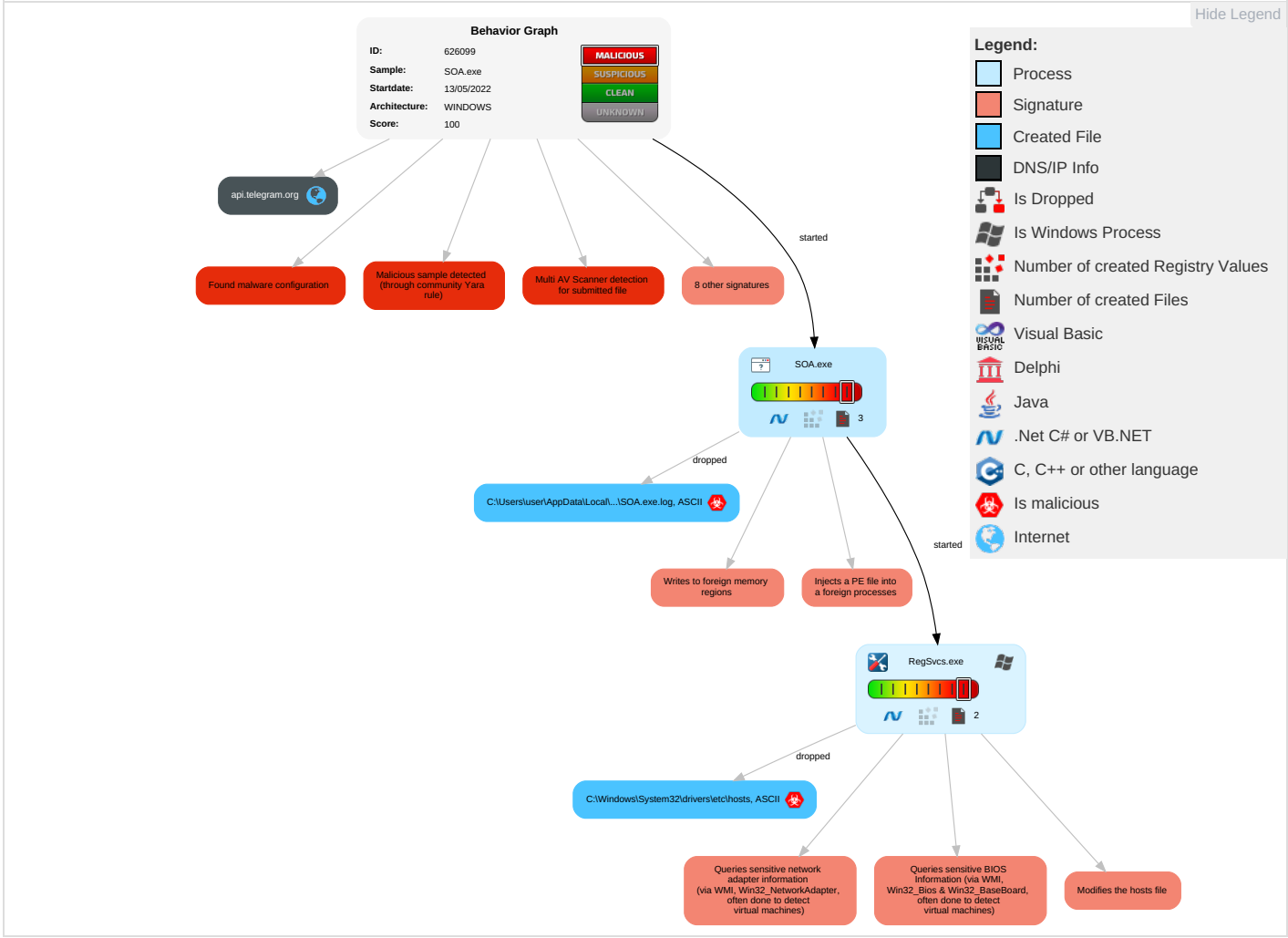
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	2 1 1 Process Injection	1 Masquerading	OS Credential Dumping	2 1 1 Security Software Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 File and Directory Permissions Modification	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Disable or Modify Tools	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 3 1 Virtualization/Sandbox Evasion	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 1 1 Process Injection	LSA Secrets	1 1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

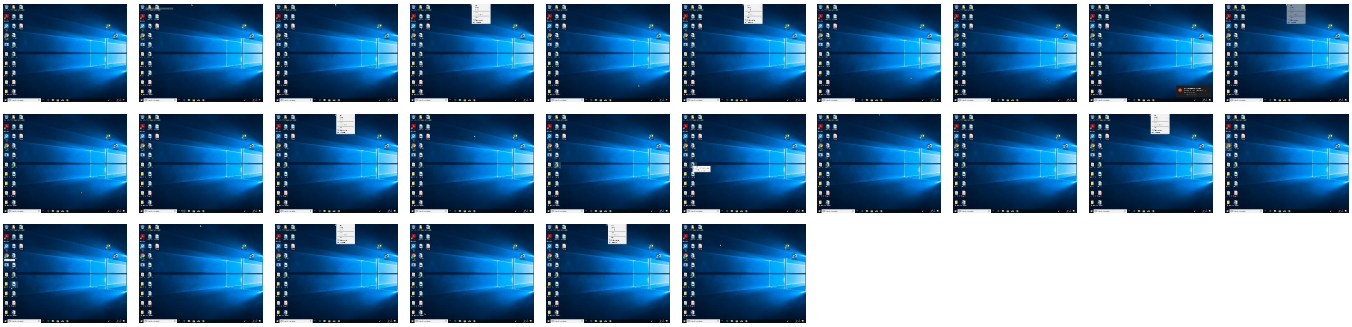
Behavior Graph



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
SOA.exe	57%	Virustotal		Browse
SOA.exe	54%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
SOA.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
6.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/lt	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://fontfabrik.comX	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comC.TTFZ	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.sakkal.comr	0%	URL Reputation	safe	
http://www.fontbureau.comgreta	0%	URL Reputation	safe	
http://www.founder.com.cn/cny	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/jp/m	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Boldv	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.founder.com.cn/cnl-s	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.fontbureau.commv	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/waS	0%	Avira URL Cloud	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://www.fontbureau.comueed	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/Z	0%	URL Reputation	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.sajatypeworks.comTF	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	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.como.F	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.sajatypeworks.com-e=n	0%	Avira URL Cloud	safe	
http://https://jkqQodeR5y.net	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/oi	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.tiro.	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.fontbureau.comdQ	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/v	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.fontbureau.comsivF	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/m	0%	URL Reputation	safe	
http://www.fontbureau.comcea	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0-e	0%	URL Reputation	safe	
http://www.fonts.com;S;	0%	Avira URL Cloud	safe	
http://www.fontbureau.comitu	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comM.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/d	0%	URL Reputation	safe	
http://https://api.telegram.org4Kl	0%	Avira URL Cloud	safe	
http://bLHfhV.com	0%	Avira URL Cloud	safe	
http://www.urwpp.deivb	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnkj	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.telegram.org	149.154.167.220	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/lt	SOA.exe, 00000000.00000003.442006747.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.442058750.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.441742704.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.441856636.0000000005528000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	RegSvcs.exe, 00000006.00000002.702221188.0000000003131000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fontfabrik.comX	SOA.exe, 00000000.00000003.435642434.000000000555D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org	RegSvcs.exe, 00000006.00000002.703086304.0000000003499000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comC.TTFZ	SOA.exe, 00000000.00000003.446934456.0000000005523000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.446256425.0000000005529000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.439443516.0000000005522000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comessed	SOA.exe, 00000000.00000003.446256425.0000000005529000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	SOA.exe, 00000000.00000003.440875113.000000000552A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	SOA.exe, 00000000.00000003.434290760.000000000553B000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.435642434.000000000555D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.comr	SOA.exe, 00000000.00000003.443375135.000000000552B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgreta	SOA.exe, 00000000.00000002.482171495.0000000005520000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.475894950.0000000005520000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cny	SOA.exe, 00000000.00000003.438672593.0000000005522000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.438684745.0000000005528000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//	SOA.exe, 00000000.00000003.441539964.0000000005523000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.441742704.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.441856636.0000000005528000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/.	SOA.exe, 00000000.00000003.442006747.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.442505928.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.441856636.0000000005528000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/m	SOA.exe, 00000000.00000003.442900542.0000000005528000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Boldv	SOA.exe, 00000000.00000003.442505928.0000000005528000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	RegSvcs.exe, 00000006.00000002.702221188.0000000003131000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.fonts.com	SOA.exe, 00000000.00000003.435412641.000000000555D000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnl-s	SOA.exe, 00000000.00000003.438383167.000000000552C000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.438258519.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.438340040.0000000005529000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	SOA.exe, 00000000.00000003.447627882.000000000552A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.commv	SOA.exe, 00000000.00000003.446256425.0000000005529000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/waS	SOA.exe, 00000000.00000003.441742704.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.441856636.0000000005528000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	RegSvcs.exe, 00000006.00000002.703086304.0000000003499000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	SOA.exe, 00000000.00000002.480070555.00000000034AF000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000006.00000002.700193844.0000000000402000.00000040.00000400.00020000.00000000.sdmp, RegSvcs.exe, 00000006.00000000.473274806.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comueed	SOA.exe, 00000000.00000003.447627882.000000000552A000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.447402029.0000000005529000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/Z	SOA.exe, 00000000.00000003.442900542.0000000005528000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnd	SOA.exe, 00000000.00000003.438406518.0000000005522000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	SOA.exe, 00000000.00000003.447627882.000000000552A000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.447402029.0000000005529000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	SOA.exe, 00000000.00000003.448559842.000000000552A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNS	RegSvcs.exe, 00000006.00000002.702221188.0000000003131000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comTF	SOA.exe, 00000000.00000003.434281330.0000000005544000.00000004.00000800.00020000.00000000.sdmp	false	• 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, 00000006.00000002.702221188.0000000003131000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot2134979594:AAFk4QkrlHlt2a-q-EhIoHZBbzxSH0QxiBI/sendDocument	RegSvcs.exe, 00000006.00000002.703086304.0000000003499000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000006.00000002.705130100.000000000630A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.como.F	SOA.exe, 00000000.00000003.440412042.000000000552A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/P	SOA.exe, 00000000.00000003.442006747.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.443375135.000000000552B000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.444062249.000000000552B000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.442900542.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.442505928.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.442058750.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.441539964.0000000005523000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.443868372.000000000552B000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.441742704.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.443934615.000000000552B000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.441856636.0000000005528000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot2134979594:AAFk4QkrlHlt2a-q-EhIoHZBbzxSH0QxiBI/	SOA.exe, 00000000.00000002.480070555.00000034AF000.00000004.00000800.00020000.00000000.sdmp, RegSvcs.exe, 00000006.00000002.700193844.0000000000402000.00000040.00000400.00020000.00000000.sdmp, RegSvcs.exe, 00000006.00000000.473274806.0000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.com-e=n	SOA.exe, 00000000.00000003.434290760.000000000553B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://jkqQodeR5y.net	RegSvcs.exe, 00000006.00000002.702221188.0000000003131000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/oi	SOA.exe, 00000000.00000003.442006747.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.442505928.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.442058750.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.441742704.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.441856636.0000000005528000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/	SOA.exe, 00000000.00000003.443934615.000000000552B000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.441856636.0000000005528000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	SOA.exe, 00000000.00000003.446256425.0000000005529000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot2134979594:AAFk4QkrlHlt2a-q-EhIoHZBbzxSH0QxiBI/sendDocumentdocument------	RegSvcs.exe, 00000006.00000002.702221188.0000000003131000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org%$	RegSvcs.exe, 00000006.00000002.702221188.0000000003131000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.	SOA.exe, 00000000.00000003.439513237.0000000005524000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.439443516.0000000005522000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	SOA.exe, 00000000.00000003.439030633.0000000005523000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	SOA.exe, 00000000.00000003.438672593.0000000005522000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.439229235.0000000005529000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.438684745.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.439030633.0000000005523000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.439157151.0000000005529000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SOA.exe, 00000000.00000003.446934456.0000000005523000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000002.482711624.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comdQ	SOA.exe, 00000000.00000003.446934456.0000000005523000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.446256425.0000000005529000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/v	SOA.exe, 00000000.00000003.442900542.0000000005528000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.monotype.	SOA.exe, 00000000.00000003.448417236.0000000005529000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comsivF	SOA.exe, 00000000.00000003.447627882.000000000552A000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.447402029.0000000005529000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/m	SOA.exe, 00000000.00000003.442006747.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.442505928.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.442058750.0000000005528000.00000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.441856636.0000000005528000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers$	SOA.exe, 00000000.00000003.447402029.0000000005529000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comcea	SOA.exe, 00000000.00000003.446256425.000 0000005529000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	SOA.exe, 00000000.00000003.442058750.000 0000005528000.00000004.00000800.00020000 .00000000.sdmp, SOA.exe, 00000000.000000 03.441539964.0000000005523000.00000004.0 0000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.441742704.00000000055 28000.00000004.00000800.00020000.0000000 0.sdmp, SOA.exe, 00000000.00000002.48271 1624.0000000006732000.00000004.00000800. 00020000.00000000.sdmp, SOA.exe, 0000000 0.00000003.441856636.0000000005528000.00 000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0-e	SOA.exe, 00000000.00000003.442900542.000 0000005528000.00000004.00000800.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com;S;	SOA.exe, 00000000.00000003.435412641.000 000000555D000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers8	SOA.exe, 00000000.00000002.482711624.000 0000006732000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://www.fontbureau.comitu	SOA.exe, 00000000.00000003.447627882.000 000000552A000.00000004.00000800.00020000 .00000000.sdmp, SOA.exe, 00000000.000000 03.447402029.0000000005529000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comals	SOA.exe, 00000000.00000003.447627882.000 000000552A000.00000004.00000800.00020000 .00000000.sdmp, SOA.exe, 00000000.000000 03.447402029.0000000005529000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comM.TTF	SOA.exe, 00000000.00000003.447627882.000 000000552A000.00000004.00000800.00020000 .00000000.sdmp, SOA.exe, 00000000.000000 03.447402029.0000000005529000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/d	SOA.exe, 00000000.00000003.442006747.000 0000005528000.00000004.00000800.00020000 .00000000.sdmp, SOA.exe, 00000000.000000 03.442900542.0000000005528000.00000004.0 0000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.442505928.00000000055 28000.00000004.00000800.00020000.0000000 0.sdmp, SOA.exe, 00000000.00000003.44205 8750.0000000005528000.00000004.00000800. 00020000.00000000.sdmp, SOA.exe, 0000000 0.00000003.441539964.0000000005523000.00 000004.00000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.441742704.000 0000005528000.00000004.00000800.00020000 .00000000.sdmp, SOA.exe, 00000000.000000 03.441856636.0000000005528000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org4Kl	RegSvcs.exe, 00000006.00000002.703086304 .0000000003499000.00000004.00000800.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://api.telegram.org	RegSvcs.exe, 00000006.00000002.703155934 .00000000034AC000.00000004.00000800.0002 0000.00000000.sdmp	false		high
http://bLHfhV.com	RegSvcs.exe, 00000006.00000002.702221188 .0000000003131000.00000004.00000800.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deivb	SOA.exe, 00000000.00000003.447627882.000 000000552A000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnkj	SOA.exe, 00000000.00000003.438383167.000 000000552C000.00000004.00000800.00020000 .00000000.sdmp, SOA.exe, 00000000.000000 03.438258519.0000000005528000.00000004.0 0000800.00020000.00000000.sdmp, SOA.exe, 00000000.00000003.438340040.00000000055 29000.00000004.00000800.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626099
Start date and time: 13/05/202215:42:10	2022-05-13 15:42:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SOA.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:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.evad.winEXE@3/2@1/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 20% • Quality standard deviation: 28.3%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:43:41	API Interceptor	1x Sleep call for process: SOA.exe modified
15:44:04	API Interceptor	610x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\SOA.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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=b77a

C:\Windows\System32\drivers\etc\hosts

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA F
Malicious:	**true**
Reputation:	high, very likely benign file

Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.018221482722969
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SOA.exe
File size:	833024
MD5:	f18604d5fc3e2930e85c403e0e80a459
SHA1:	aa0517c10c333f9a9a64eba154ea915464ebf2bb
SHA256:	46584937f3c753886bb38030047dd11c73d46bf01c5e52a95118108634ee2081
SHA512:	c39bd01bca62779434b0508bc66972cd7030153469f631b425e1b77af59fd7db1a26a837ea2b7440c9f93cd538c43c2f2005ebcf34b982c03ceed71a4c3b685c
SSDEEP:	12288:7HE2ISZ5m4fuOjUTPXmkHz/b9m+DhLrRvoXSf+bnl8tTac2aVzBQXOCmxqogCSsV:b3NUXmkTjZFRvoCmblML
TLSH:	1705A59C722831DFC85BD276DAA81C68EA90757F931F5103A02715AD9A1CAC7EF148F3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....|b.....P..... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4cc11e
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:	0x627C8C90 [Thu May 12 04:26:56 2022 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xcc0cc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xce000	0xf00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xca124	0xca200	False	0.611404220779	data	7.02001355184	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xce000	0xf00	0x1000	False	0.35791015625	data	4.853048536	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd0000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xce0a0	0x348	data		
RT_MANIFEST	0xce3e8	0xb15	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2022
Assembly Version	1.0.0.0
InternalName	x2pyR.exe
FileVersion	1.0.0.0
CompanyName	Bean Cafe
LegalTrademarks	
Comments	
ProductName	Managerial and Cashier Screens
ProductVersion	1.0.0.0
FileDescription	Bean Cafe
OriginalFilename	x2pyR.exe

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 15:45:33.422219992 CEST	50668	53	192.168.2.5	8.8.8.8
May 13, 2022 15:45:33.441097021 CEST	53	50668	8.8.8.8	192.168.2.5

DNS Queries

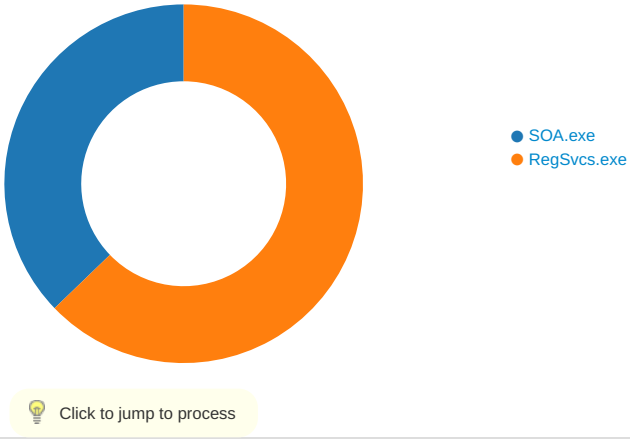
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 13, 2022 15:45:33.422219992 CEST	192.168.2.5	8.8.8.8	0x92a0	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2022 15:45:33.441097021 CEST	8.8.8.8	192.168.2.5	0x92a0	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: SOA.exe PID: **6968**, Parent PID: **6000**

General

Target ID:	0
Start time:	15:43:24
Start date:	13/05/2022
Path:	C:\Users\user\Desktop\SOA.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SOA.exe"
Imagebase:	0x110000
File size:	833024 bytes
MD5 hash:	F18604D5FC3E2930E85C403E0E80A459
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: 00000000.00000002.480070555.00000000034AF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.480070555.00000000034AF000.00000004.00000800.00020000.00000000.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	6E31CF06	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	6E31CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SOA.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E62C78D	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\SOA.exe.log	0	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",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"," C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E62C907	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	6E2F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E2F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E2FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E2503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E2F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E2F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D161B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D161B4F	ReadFile

Analysis Process: RegSvcs.exe PID: **6360**, Parent PID: **6968**

General

Target ID:	6
Start time:	15:43:44
Start date:	13/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xdf0000
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: 00000006.00000002.700193844.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.700193844.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.474512000.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.474512000.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.474083361.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.474083361.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.473274806.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.473274806.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.473700502.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.473700502.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.702221188.0000000003131000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000006.00000002.702221188.0000000003131000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.702221188.0000000003131000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000006.00000002.702221188.0000000003131000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
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	6E31CF06	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	6E31CF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	824	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	127.0.0.1	success or wait	1	6D161B4F	WriteFile

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	6E2F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E2F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E2F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E2F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E2FCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E2FCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E2FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E2503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E2F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E2F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D161B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D161B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6D161B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6D161B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E2F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E2F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D161B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D161B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6D161B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6D161B4F	ReadFile

Disassembly

No disassembly