ID: 383988
Sample Name: svchost[1].exe
Cookbook: default.jbs
Time: 13:42:42
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

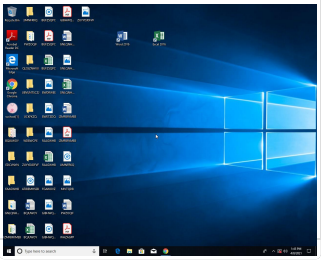
Analysis Report svchost[1].exe

Overview

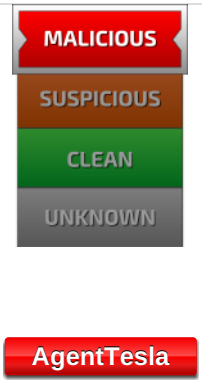
General Information

Sample Name:	svchost[1].exe
Analysis ID:	383988
MD5:	f31b0e7d038ed9d.
SHA1:	a4311ea256fb28f..
SHA256:	30865d42d9897a..
Infos:	

Most interesting Screenshot:



Detection



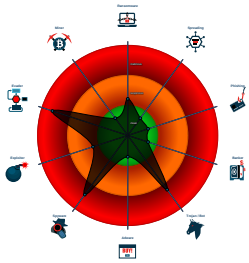
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…

Classification



Startup

- **System is w10x64**
- svchost[1].exe (PID: 6956 cmdline: 'C:\Users\user\Desktop\svchost[1].exe' MD5: F31B0E7D038ED9D64BE2C6EF94FA5171)
  - svchost[1].exe (PID: 5872 cmdline: C:\Users\user\Desktop\svchost[1].exe MD5: F31B0E7D038ED9D64BE2C6EF94FA5171)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "helio@lpsinvest.comz6~Rhjss*B0}smtp.lpsinvest.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.907761661.000000000307 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000000.00000002.666294047.0000000003A3 C000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.906186292.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.665319943.0000000002A8 4000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.667204898.0000000003C5 A000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 4 entries

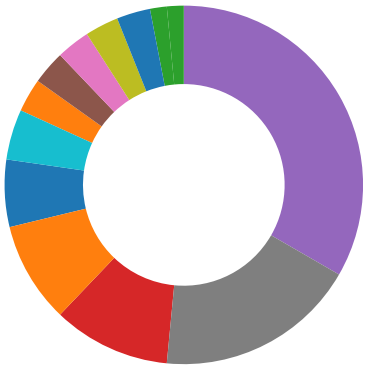
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.svchost[1].exe.3c80048.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.2.svchost[1].exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.svchost[1].exe.3b49d80.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.svchost[1].exe.3b49d80.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

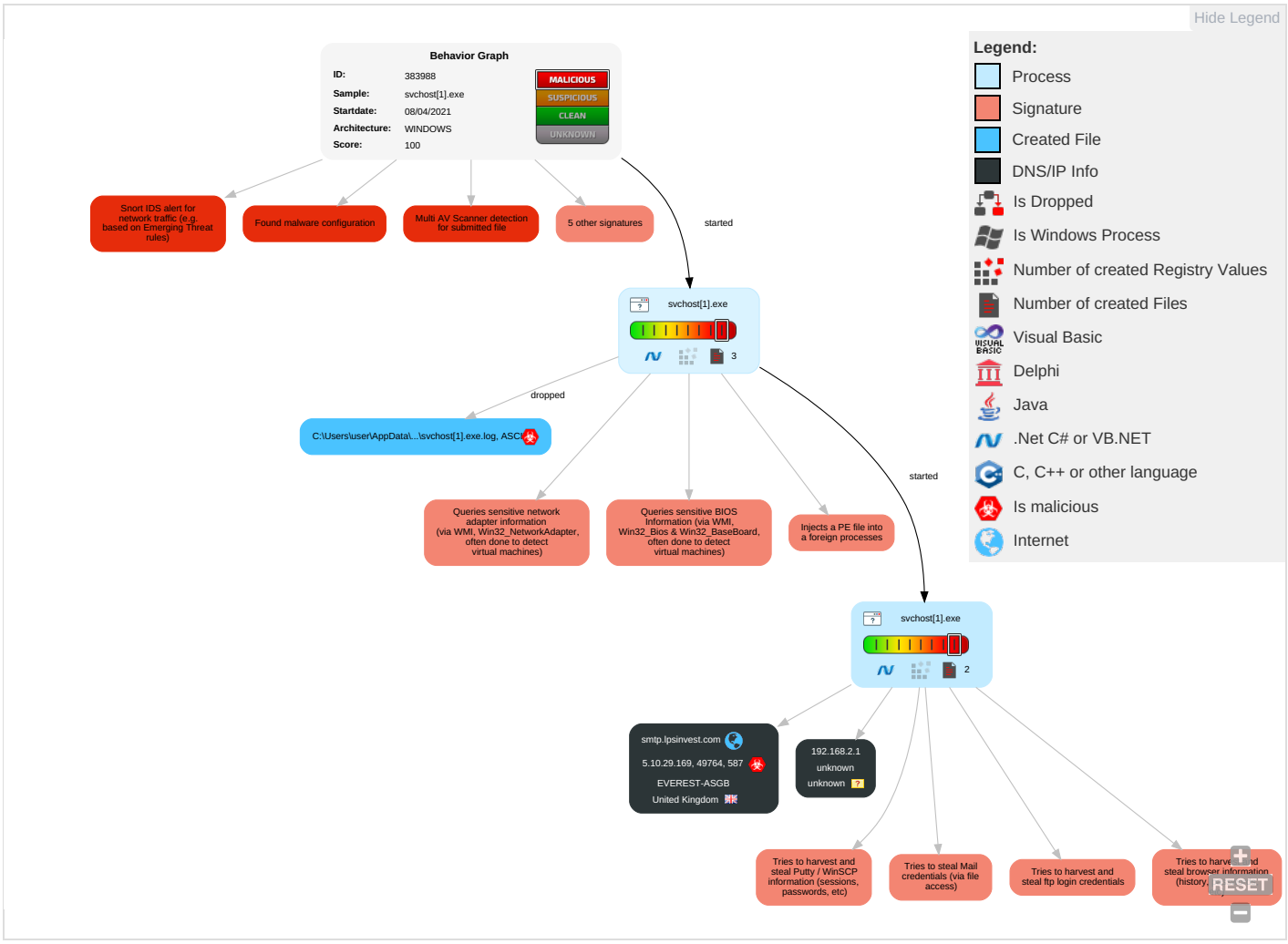
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

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

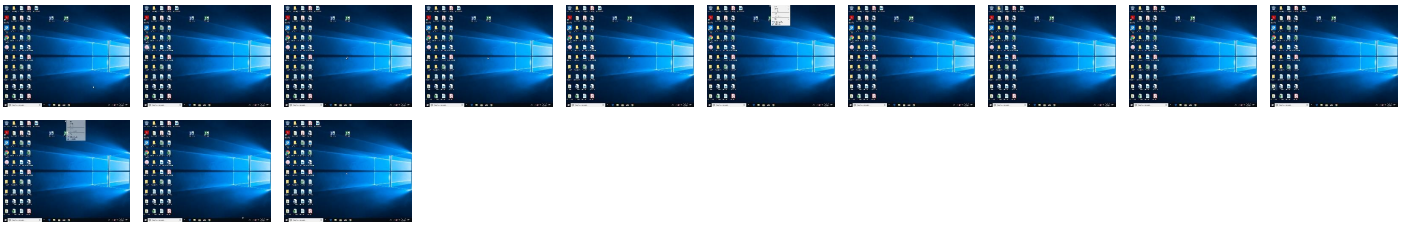
Behavior Graph



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
svchost[1].exe	16%	Virustotal		Browse
svchost[1].exe	17%	ReversingLabs	Win32.Trojan.AgentTesla	
svchost[1].exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.svchost[1].exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.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://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.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.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	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.sandoll.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnZ	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.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.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://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	

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://97E09xoEksglOT.net	0%	Avira URL Cloud	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	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.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://https://api.ipify.org%$	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.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.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn0	0%	Avira URL Cloud	safe	
http://smtp.lpsinvest.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://AFplKq.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.lpsinvest.com	5.10.29.169	true	true		unknown

URLs from Memory and Binaries

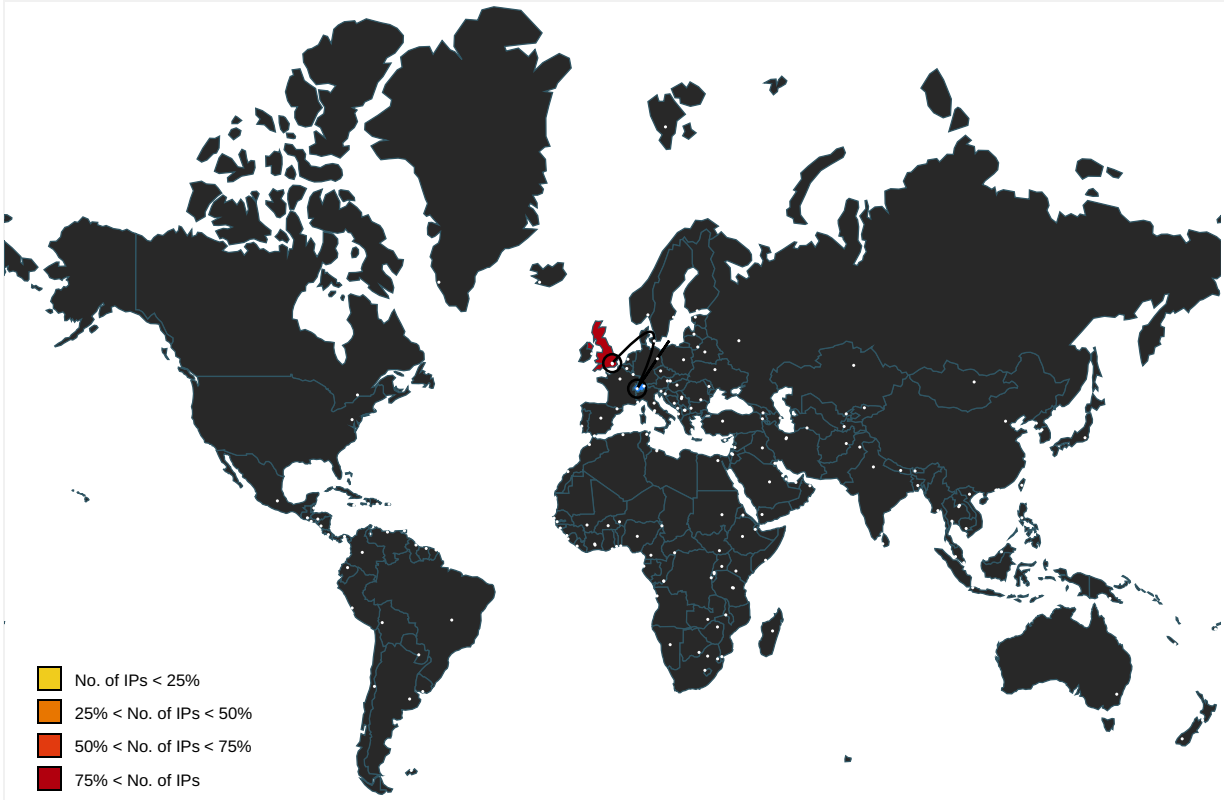
Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	svchost[1].exe, 00000005.00000002.907761661.0000000003071000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dist.nuget.org/win-x86-commandline/latest/nuget.exe	svchost[1].exe	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name4	svchost[1].exe, 00000000.00000002.665335915.0000000002A8B000.00000004.00000001.sdmp	false		high
http://www.tiro.com	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	svchost[1].exe, 00000000.00000002.665319943.0000000002A84000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp, svchost[1].exe, 00000000.00000003.644385711.0000000005AD3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	svchost[1].exe, 00000005.00000002.907761661.0000000003071000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.ascendercorp.com/typedesigners.html	svchost[1].exe, 00000000.00000003.649388172.0000000005B0D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Spegeli/Pokemon-Go-Rocket-API/archive/master.zip	svchost[1].exe	false		high
http://www.fonts.com	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnZ	svchost[1].exe, 00000000.00000003.647133595.0000000005AD7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	svchost[1].exe, 00000000.00000002.665163215.0000000002A31000.00000004.00000001.sdmp, svchost[1].exe, 00000000.00000002.665335915.0000000002A8B000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.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	svchost[1].exe, 00000000.00000002.666294047.0000000003A3C000.00000004.00000001.sdmp, svchost[1].exe, 00000005.00000002.906186292.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://97E09xoEksglOT.net	svchost[1].exe, 00000005.00000002.908431013.00000000033D4000.00000004.00000001.sdmp, svchost[1].exe, 00000005.00000002.908461023.00000000033E4000.00000004.00000001.sdmp, svchost[1].exe, 00000005.00000002.908377566.000000000339D000.00000004.00000001.sdmp, svchost[1].exe, 00000005.00000002.908473952.00000000033EA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com=	svchost[1].exe, 00000000.00000002.669535009.0000000005AD0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	svchost[1].exe, 00000000.00000002.669535009.0000000005AD0000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	svchost[1].exe, 00000005.00000002.907761661.0000000003071000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.comt	svchost[1].exe, 00000000.00000003.644385711.0000000005AD3000.00000004.00000001.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	svchost[1].exe, 00000005.00000002.907761661.0000000003071000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/d-haxton/HaxtonBot/archive/master.zip	svchost[1].exe	false		high
http://www.fontbureau.coma	svchost[1].exe, 00000000.00000002.669535009.0000000005AD0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%$	svchost[1].exe, 00000005.00000002.907761661.0000000003071000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	svchost[1].exe, 00000000.00000003.647329385.0000000005AD8000.00000004.00000001.sdmp, svchost[1].exe, 00000000.00000003.647395558.0000000005AD6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn	svchost[1].exe, 00000000.00000003.647133595.0000000005AD7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn0	svchost[1].exe, 00000000.00000003.647133595.0000000005AD7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false		high
http://smtp.lpsinvest.com	svchost[1].exe, 00000005.00000002.908445459.00000000033DA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://AFplKq.com	svchost[1].exe, 00000005.00000002.907761661.0000000003071000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	svchost[1].exe, 00000000.00000002.670258477.0000000006CE2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnd:	svchost[1].exe, 00000000.00000003.646976353.0000000005ADE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.10.29.169	smtp.lpsinvest.com	United Kingdom		60610	EVEREST-ASGB	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383988
Start date:	08.04.2021
Start time:	13:42:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	svchost[1].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:	20
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@1/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 17.8% • Quality standard deviation: 31.4%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 23.54.113.53, 52.147.198.201, 52.255.188.83, 20.50.102.62, 23.10.249.26, 23.10.249.43, 13.88.21.125, 52.155.217.156, 20.54.26.129, 20.82.210.154, 104.43.193.48 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.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
13:43:36	API Interceptor	720x Sleep call for process: svchost[1].exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
5.10.29.169	PAGO.xlsx	Get hash	malicious	Browse	
	78jqVxp7pl.exe	Get hash	malicious	Browse	
	AhJ6Pqv5Ik.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.598.11918.exe	Get hash	malicious	Browse	
	179422427-105719-sanlccjavap0003-1.pdf.exe	Get hash	malicious	Browse	
	6wYAsx4N91.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Win32.Save.a.2641.exe	Get hash	malicious	Browse	
	Transf. ppto 310404.xlsx	Get hash	malicious	Browse	
	PAGO.xlsx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.lpsinvest.com	PAGO.xlsx	Get hash	malicious	Browse	• 5.10.29.169
	78jqVxp7pl.exe	Get hash	malicious	Browse	• 5.10.29.169

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EVEREST-ASGB	PAGO.xlsx	Get hash	malicious	Browse	• 5.10.29.169
	78jqVxp7pl.exe	Get hash	malicious	Browse	• 5.10.29.169
	AhJ6Pqv5Ik.exe	Get hash	malicious	Browse	• 5.10.29.169
	SecuriteInfo.com.Trojan.PackedNET.598.11918.exe	Get hash	malicious	Browse	• 5.10.29.169
	179422427-105719-sanlccjavap0003-1.pdf.exe	Get hash	malicious	Browse	• 5.10.29.169
	6wYAsx4N91.exe	Get hash	malicious	Browse	• 5.10.29.169
	SecuriteInfo.com.Trojan.Win32.Save.a.2641.exe	Get hash	malicious	Browse	• 5.10.29.169
	Transf. ppto 310404.xlsx	Get hash	malicious	Browse	• 5.10.29.169
	PAGO.xlsx	Get hash	malicious	Browse	• 5.10.29.169

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\svchost[1].exe.log

Process:	C:\Users\user\Desktop\svchost[1].exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\svchost[1].exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.231779565509928
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:	svchost[1].exe
File size:	908800
MD5:	f31b0e7d038ed9d64be2c6ef94fa5171
SHA1:	a4311ea256fb28fa7815249f43c903641c7114da
SHA256:	30865d42d9897a6611df8683bc041836794cf6d7ee47763281fbed0f063a7c8e
SHA512:	45c21e3bf159c80ed6978a92134397074cafec0e523966c5c691ef3769764209922fec772612c61e12d45a3c157e69264c3bcd89d3cd1ec142778e42b76de01
SSDEEP:	12288:SSLIIK2eESKnuHOvMUUzui2KrbCR4MzRBMuWRTIv/YLOn8gsIKUvE+:SSEIVfuuU/zbCxz4FYwankIc
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...y.n`.....P.....F..... .....@.. .....@.....@.....

File Icon

Icon Hash:	e8d4ae708e8ec461

Static PE Info

General

Entrypoint:	0x4ab49a
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:	0x606EB279 [Thu Apr 8 07:36:25 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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	0xab448	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xac000	0x34234	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe2000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa94a0	0xa9600	False	0.794058464022	data	7.56739593384	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xac000	0x34234	0x34400	False	0.389905427632	data	5.76174565278	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xac220	0x521e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xb1450	0x6f5a	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xb83bc	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xc8bf4	0x94a8	data		
RT_ICON	0xd20ac	0x5488	data		
RT_ICON	0xd7544	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 15794175, next used block 4294902528		
RT_ICON	0xdb77c	0x25a8	data		
RT_ICON	0xddd34	0x10a8	data		
RT_ICON	0xdedec	0x988	data		
RT_ICON	0xdf784	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xdfbfc	0x92	data		
RT_VERSION	0xdfca0	0x392	data		
RT_MANIFEST	0xe0044	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 2016 Computer City
Assembly Version	1.12.0.2
InternalName	CreateRangesd9.exe
FileVersion	1.12.0.2
CompanyName	Computer City
LegalTrademarks	
Comments	
ProductName	UnmanagedAccessor
ProductVersion	1.12.0.2
FileDescription	UnmanagedAccessor
OriginalFilename	CreateRangesd9.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-13:45:21.100935	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49764	587	192.168.2.4	5.10.29.169

Network Port Distribution

Total Packets: 52

- 53 (DNS)
- 587 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:45:20.774466991 CEST	49764	587	192.168.2.4	5.10.29.169
Apr 8, 2021 13:45:20.809410095 CEST	587	49764	5.10.29.169	192.168.2.4
Apr 8, 2021 13:45:20.809658051 CEST	49764	587	192.168.2.4	5.10.29.169
Apr 8, 2021 13:45:20.843045950 CEST	587	49764	5.10.29.169	192.168.2.4
Apr 8, 2021 13:45:20.843540907 CEST	49764	587	192.168.2.4	5.10.29.169
Apr 8, 2021 13:45:20.876821041 CEST	587	49764	5.10.29.169	192.168.2.4
Apr 8, 2021 13:45:20.878261089 CEST	49764	587	192.168.2.4	5.10.29.169
Apr 8, 2021 13:45:20.911379099 CEST	587	49764	5.10.29.169	192.168.2.4
Apr 8, 2021 13:45:20.911873102 CEST	49764	587	192.168.2.4	5.10.29.169
Apr 8, 2021 13:45:20.945014954 CEST	587	49764	5.10.29.169	192.168.2.4
Apr 8, 2021 13:45:20.945971012 CEST	49764	587	192.168.2.4	5.10.29.169
Apr 8, 2021 13:45:20.980176926 CEST	587	49764	5.10.29.169	192.168.2.4
Apr 8, 2021 13:45:20.982388020 CEST	49764	587	192.168.2.4	5.10.29.169
Apr 8, 2021 13:45:21.016210079 CEST	587	49764	5.10.29.169	192.168.2.4
Apr 8, 2021 13:45:21.016686916 CEST	49764	587	192.168.2.4	5.10.29.169
Apr 8, 2021 13:45:21.099493027 CEST	587	49764	5.10.29.169	192.168.2.4
Apr 8, 2021 13:45:21.100934982 CEST	49764	587	192.168.2.4	5.10.29.169
Apr 8, 2021 13:45:21.101042986 CEST	49764	587	192.168.2.4	5.10.29.169
Apr 8, 2021 13:45:21.101499081 CEST	49764	587	192.168.2.4	5.10.29.169
Apr 8, 2021 13:45:21.101574898 CEST	49764	587	192.168.2.4	5.10.29.169
Apr 8, 2021 13:45:21.134054899 CEST	587	49764	5.10.29.169	192.168.2.4
Apr 8, 2021 13:45:21.134463072 CEST	587	49764	5.10.29.169	192.168.2.4
Apr 8, 2021 13:45:21.134802103 CEST	587	49764	5.10.29.169	192.168.2.4
Apr 8, 2021 13:45:21.174755096 CEST	49764	587	192.168.2.4	5.10.29.169

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:43:21.360517979 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:43:21.373454094 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 8, 2021 13:43:22.819057941 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:43:22.838268995 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 8, 2021 13:43:36.506131887 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:43:36.518707991 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 8, 2021 13:43:44.738883972 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:43:44.751890898 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 8, 2021 13:43:46.826216936 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:43:46.839076042 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 8, 2021 13:43:47.449106932 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:43:47.462033987 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 8, 2021 13:43:48.538242102 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:43:48.551193953 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 8, 2021 13:43:49.187021017 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:43:49.200397968 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 8, 2021 13:43:54.371588945 CEST	63153	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:43:54.384330034 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 8, 2021 13:43:58.241430044 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:43:58.260020971 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:02.131122112 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:02.143009901 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:02.813589096 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:02.826136112 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:03.807391882 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:03.820637941 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:05.897753000 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:05.910046101 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:06.852571011 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:06.865803957 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:10.494389057 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:10.507993937 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:11.561630011 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:11.660725117 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:12.150500059 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:12.178684950 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:12.191378117 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:12.392133951 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:12.849486113 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:12.992903948 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:13.263180017 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:13.289325953 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:13.376241922 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:13.389256001 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:13.793956995 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:13.807368994 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:14.212326050 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:15.216603994 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:15.349567890 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:15.696815968 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:15.709959984 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:16.316134930 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:16.329654932 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:17.454092026 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:17.467392921 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:18.156184912 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:18.169085026 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:21.910017014 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:21.922573090 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:22.993221045 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:23.005882025 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:24.075020075 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:24.087544918 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:28.624958038 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:28.660696983 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:29.063834906 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:29.079916000 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:30.455490112 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:30.467747927 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 8, 2021 13:44:31.131867886 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:44:31.145515919 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 8, 2021 13:45:03.703135967 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:45:03.735781908 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 8, 2021 13:45:05.588020086 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:45:05.601299047 CEST	53	55916	8.8.8.8	192.168.2.4
Apr 8, 2021 13:45:20.593401909 CEST	52752	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:45:20.638649940 CEST	53	52752	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 13:45:20.593401909 CEST	192.168.2.4	8.8.8.8	0x2ebe	Standard query (0)	smtp.lpsinvest.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:45:20.638649940 CEST	8.8.8.8	192.168.2.4	0x2ebe	No error (0)	smtp.lpsinvest.com		5.10.29.169	A (IP address)	IN (0x0001)

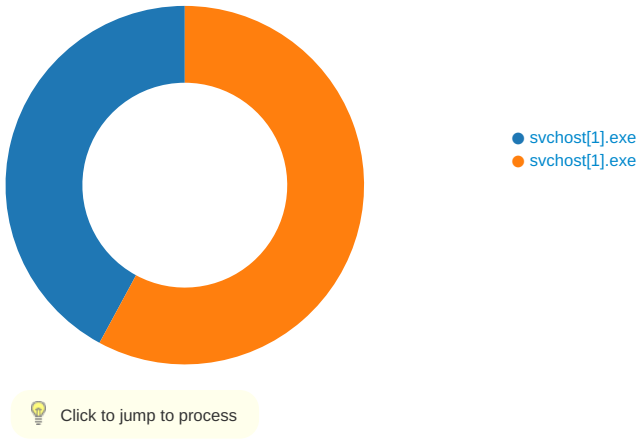
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 8, 2021 13:45:20.843045950 CEST	587	49764	5.10.29.169	192.168.2.4	220 mail.elixir.eu.com
Apr 8, 2021 13:45:20.843540907 CEST	49764	587	192.168.2.4	5.10.29.169	EHLO 284992
Apr 8, 2021 13:45:20.876821041 CEST	587	49764	5.10.29.169	192.168.2.4	250-mail.elixir.eu.com Hello [185.32.222.8] 250-SIZE 31457280 250-AUTH LOGIN CRAM-MD5 250-STARTTLS 250-8BITMIME 250 OK
Apr 8, 2021 13:45:20.878261089 CEST	49764	587	192.168.2.4	5.10.29.169	AUTH login aGVsaW9AbHBzaW52ZXN0LmNvbQ==
Apr 8, 2021 13:45:20.911379099 CEST	587	49764	5.10.29.169	192.168.2.4	334 UGFzc3dvcmQ6
Apr 8, 2021 13:45:20.945014954 CEST	587	49764	5.10.29.169	192.168.2.4	235 Authentication successful
Apr 8, 2021 13:45:20.945971012 CEST	49764	587	192.168.2.4	5.10.29.169	MAIL FROM:<helio@lpsinvest.com>
Apr 8, 2021 13:45:20.980176926 CEST	587	49764	5.10.29.169	192.168.2.4	250 OK <helio@lpsinvest.com> Sender ok
Apr 8, 2021 13:45:20.982388020 CEST	49764	587	192.168.2.4	5.10.29.169	RCPT TO:<helio@lpsinvest.com>
Apr 8, 2021 13:45:21.016210079 CEST	587	49764	5.10.29.169	192.168.2.4	250 OK <helio@lpsinvest.com> Recipient ok
Apr 8, 2021 13:45:21.016686916 CEST	49764	587	192.168.2.4	5.10.29.169	DATA
Apr 8, 2021 13:45:21.099493027 CEST	587	49764	5.10.29.169	192.168.2.4	354 Start mail input; end with <CRLF>.<CRLF>
Apr 8, 2021 13:45:21.101574898 CEST	49764	587	192.168.2.4	5.10.29.169	.
Apr 8, 2021 13:45:21.134802103 CEST	587	49764	5.10.29.169	192.168.2.4	250 OK

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: svchost[1].exe PID: 6956 Parent PID: 5944

General

Start time:	13:43:27
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\svchost[1].exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\svchost[1].exe'
Imagebase:	0x670000
File size:	908800 bytes
MD5 hash:	F31B0E7D038ED9D64BE2C6EF94FA5171
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: 00000000.00000002.666294047.0000000003A3C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.665319943.0000000002A84000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.667204898.0000000003C5A000.00000004.00000001.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	6D38CF06	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	6D38CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\svchost[1].exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\svchost[1].exe.log	unknown	1314	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D69C907	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile

Analysis Process: svchost[1].exe PID: 5872 Parent PID: 6956

General

Start time:	13:43:37
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\svchost[1].exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\svchost[1].exe
Imagebase:	0xad0000
File size:	908800 bytes
MD5 hash:	F31B0E7D038ED9D64BE2C6EF94FA5171
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.907761661.0000000003071000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.906186292.0000000000402000.00000040.00000001.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	6D38CF06	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	6D38CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\d5be1e9a-f49c-46de-9eff-f12c4fa91692	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C1D1B4F	ReadFile

Disassembly

Code Analysis