ID: 404156
Sample Name:
ATuRNgegI7kl7Ua.exe
Cookbook: default.jbs
Time: 18:58:53
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

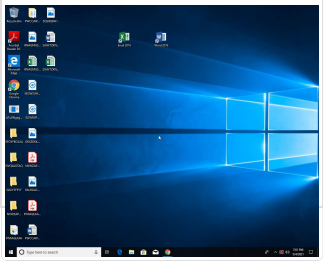
Analysis Report ATuRNgegI7kl7Ua.exe

Overview

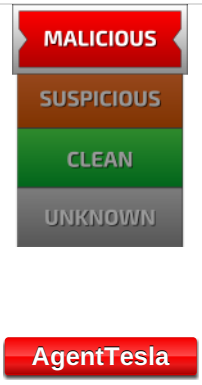
General Information

Sample Name:	ATuRNgegI7kl7Ua.exe
Analysis ID:	404156
MD5:	ec217acdf26636d..
SHA1:	768c321ffe79e38..
SHA256:	e27c7feb3112b0f..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection



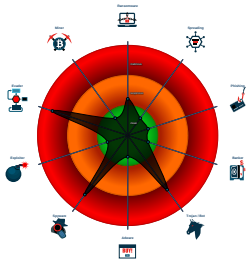
AgentTesla

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

Signatures

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

Classification



Startup

- **System is w10x64**
- ATuRNgegI7kl7Ua.exe (PID: 5856 cmdline: 'C:\Users\user\Desktop\ATuRNgegI7kl7Ua.exe' MD5: EC217ACDF26636DD01CCBA3DC7DF5066)
  - ATuRNgegI7kl7Ua.exe (PID: 1368 cmdline: C:\Users\user\Desktop\ATuRNgegI7kl7Ua.exe MD5: EC217ACDF26636DD01CCBA3DC7DF5066)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "victo@chefoowork.comYi-yIzLFE-*bmail.chefoowork.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.480281925.0000000002E11000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.480281925.0000000002E11000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000004.00000002.475257684.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.239732017.0000000003F39000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.235727199.0000000002FAC000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Click to see the 4 entries

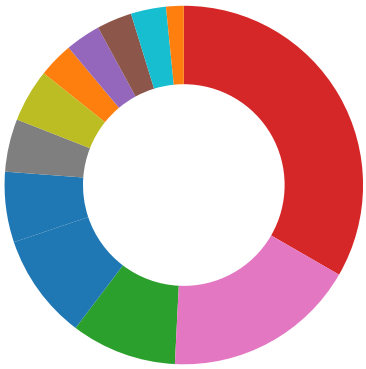
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.ATuRNgegI7kl7Ua.exe.4045970.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.ATuRNgegI7kl7Ua.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.ATuRNgegI7kl7Ua.exe.4045970.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

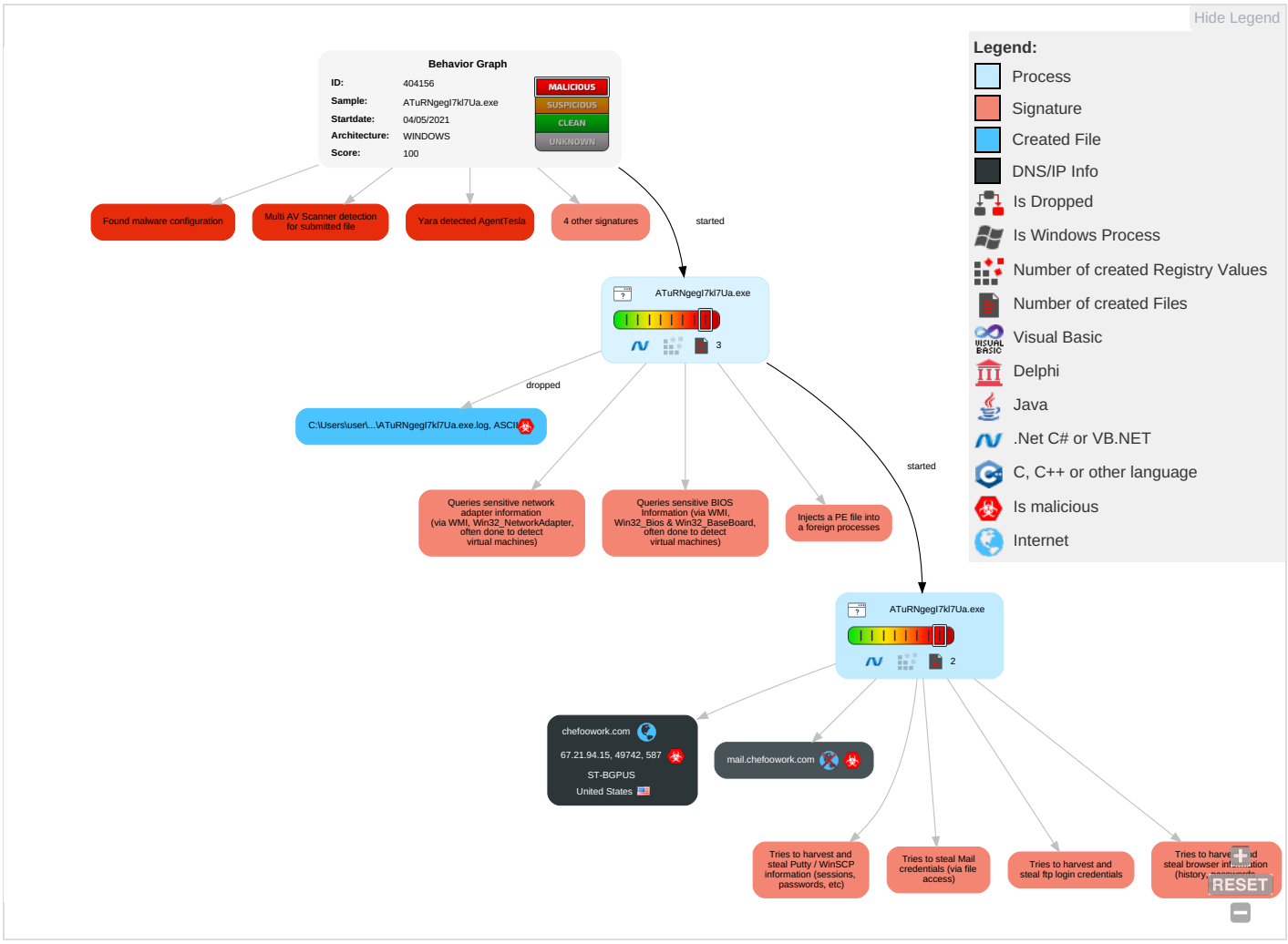
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	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 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband 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

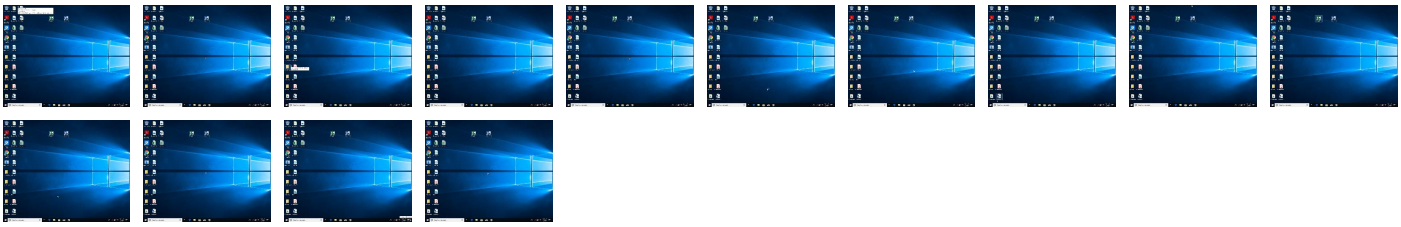
Behavior Graph



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
ATuRNgegI7kl7Ua.exe	21%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
ATuRNgegI7kl7Ua.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.ATuRNgegI7kl7Ua.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
chefoowork.com	0%	Virustotal		Browse
mail.chefoowork.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnN	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.fontbureau.comldvan	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://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://chefoowork.com	0%	Virustotal		Browse
http://chefoowork.com	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	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.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.tiro.comtnP	0%	Avira URL Cloud	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.sandoll.co.krP	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.carterandcone.comP	0%	Avira URL Cloud	safe	
http://www.churchsw.org/church-projector-project	0%	Avira URL Cloud	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.krF	0%	URL Reputation	safe	
http://www.sandoll.co.krF	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.krF	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.sandoll.co.krormal	0%	Avira URL Cloud	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.carterandcone.com=k(	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://H5aErSJgJW.org	0%	Avira URL Cloud	safe	
http://kFANsF.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	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.sandoll.co.krimP	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	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.churchsw.org/repository/Bibles/	0%	Avira URL Cloud	safe	
http://mail.chefoowork.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmn	0%	Avira URL Cloud	safe	
http://crt.comodoca	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn)	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
chefoowork.com	67.21.94.15	true	true	• 0%, Virustotal, Browse	unknown
mail.chefoowork.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

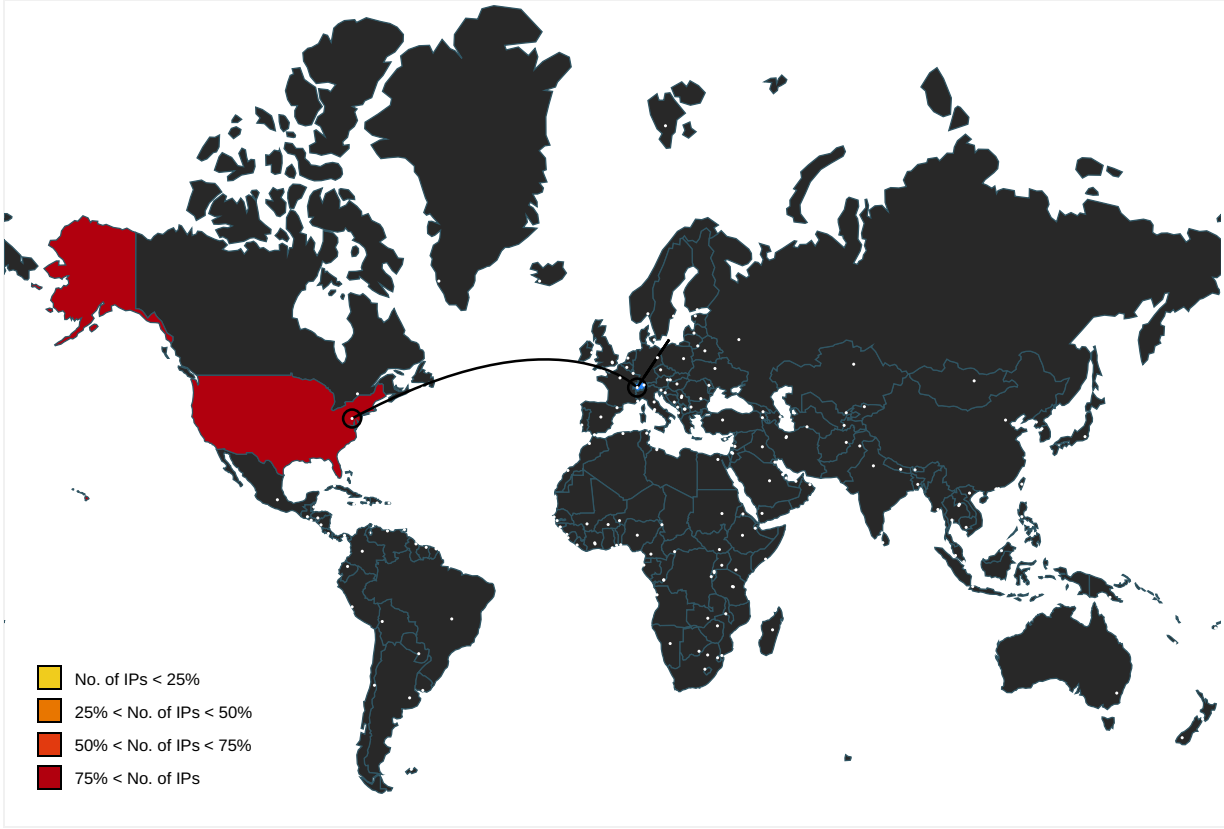
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersBo	ATuRNgegI7kl7Ua.exe, 00000000.00000003.215126918.00000000060D5000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersco	ATuRNgegI7kl7Ua.exe, 00000000.00000003.222970335.00000000060D5000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnN	ATuRNgegI7kl7Ua.exe, 00000000.00000003.212255802.00000000060AF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	ATuRNgegI7kl7Ua.exe, 00000004.00000002.480281925.0000000002E11000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.000000006190000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersF	ATuRNgegI7kl7Ua.exe, 00000000.00000003.215126918.000000006D5000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comldvan	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244672949.000000006A0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comn-u	ATuRNgegI7kl7Ua.exe, 00000000.00000003.212707591.000000006A3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.000000006190000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.000000006190000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.000000006190000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersersto	ATuRNgegI7kl7Ua.exe, 00000000.00000003.214795644.000000006D5000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersB	ATuRNgegI7kl7Ua.exe, 00000000.00000003.222970335.000000006D5000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersto	ATuRNgegI7kl7Ua.exe, 00000000.00000003.216085467.000000006D5000.00000004.00000001.sdmp	false		high
http://www.tiro.com	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.000000006190000.00000002.00000001.sdmp, ATuRNgegI7kl7Ua.exe, 00000000.00000003.212707591.000000006A3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://chefoowork.com	ATuRNgegI7kl7Ua.exe, 00000004.00000002.482432785.000000003BBC000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/P	ATuRNgegI7kl7Ua.exe, 00000000.00000003.214709420.000000006AC000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.000000006190000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	ATuRNgegI7kl7Ua.exe, 00000000.00000003.211933873.000000006B0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	ATuRNgegI7kl7Ua.exe, 00000000.00000003.213030960.000000006A4000.00000004.00000001.sdmp, ATuRNgegI7kl7Ua.exe, 00000000.00000003.212707591.000000006A3000.00000004.00000001.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	ATuRNgegI7kl7Ua.exe, 00000000.00000002.235727199.0000000002FAC000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers6o	ATuRNgegI7kl7Ua.exe, 00000000.00000003.216371701.000000006D5000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.000000006190000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.000000006190000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.000000006190000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	ATuRNgegI7kl7Ua.exe, 00000000.00000003.222533395.00000000060E6000.00000004.00000001.sdmp, ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.0000000006190000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.0000000006190000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comgrita	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244672949.00000000060A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comtnP	ATuRNgegI7kl7Ua.exe, 00000000.00000003.210857080.00000000060BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comC	ATuRNgegI7kl7Ua.exe, 00000000.00000003.212738820.00000000060A3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krP	ATuRNgegI7kl7Ua.exe, 00000000.00000003.211933873.00000000060B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers(o	ATuRNgegI7kl7Ua.exe, 00000000.00000003.214734850.00000000060D5000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.0000000006190000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comP	ATuRNgegI7kl7Ua.exe, 00000000.00000003.212656056.00000000060A3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.churchsw.org/church-projector-project	ATuRNgegI7kl7Ua.exe	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	ATuRNgegI7kl7Ua.exe, 00000000.00000003.210334592.00000000060BB000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	ATuRNgegI7kl7Ua.exe, 00000000.00000003.211933873.00000000060B0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krF	ATuRNgegI7kl7Ua.exe, 00000000.00000003.211933873.00000000060B0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.0000000006190000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krormal	ATuRNgegI7kl7Ua.exe, 00000000.00000003.211933873.00000000060B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.0000000006190000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com=k(	ATuRNgegI7kl7Ua.exe, 00000000.00000003.212707591.00000000060A3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	ATuRNgegI7kl7Ua.exe, 00000000.00000002.235516874.0000000002F31000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.0000000006190000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	ATuRNgegI7kl7Ua.exe, 00000000.00000002.239732017.0000000003F39000.00000004.00000001.sdmp, ATuRNgegI7kl7Ua.exe, 00000004.00000002.475257684.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlm	ATuRNgegI7kl7Ua.exe, 00000000.00000003.215924440.00000000060AC000.00000004.00000001.sdmp	false		high
http://H5aErSJgJW.org	ATuRNgegI7kl7Ua.exe, 00000004.00000002.482397144.00000000030B4000.00000004.00000001.sdmp, ATuRNgegI7kl7Ua.exe, 00000004.00000002.480281925.0000000002E11000.00000004.00000001.sdmp, ATuRNgegI7kl7Ua.exe, 00000004.00000002.482558346.00000000030E6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://kFANsF.com	ATuRNgegI7kl7Ua.exe, 00000004.00000002.480281925.0000000002E11000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.0000000006190000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.0000000006190000.00000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/	ATuRNgegI7kl7Ua.exe, 00000000.00000003.217799053.00000000060AC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://DynDns.comDynDNS	ATuRNgegI7kl7Ua.exe, 00000004.00000002.480281925.0000000002E11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.htmlh	ATuRNgegI7kl7Ua.exe, 00000000.00000003.215586670.00000000060AC000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.krimP	ATuRNgegI7kl7Ua.exe, 00000000.00000003.211933873.00000000060B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0	ATuRNgegI7kl7Ua.exe, 00000004.00000002.485921088.0000000006860000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	ATuRNgegI7kl7Ua.exe, 00000004.00000002.480281925.0000000002E11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.churchsw.org/repository/Bibles/	ATuRNgegI7kl7Ua.exe	false	• Avira URL Cloud: safe	unknown
http://mail.chefoowork.com	ATuRNgegI7kl7Ua.exe, 00000004.00000002.482432785.00000000030BC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmn	ATuRNgegI7kl7Ua.exe, 00000000.00000003.218026145.00000000060AC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.comodoca	ATuRNgegI7kl7Ua.exe, 00000004.00000002.485921088.0000000006860000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comn)	ATuRNgegI7kl7Ua.exe, 00000000.00000003.213030960.00000000060A4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.0000000006190000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.0000000006190000.00000002.00000001.sdmp, ATuRNgegI7kl7Ua.exe, 00000000.00000003.215924440.00000000060AC000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.0000000006190000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.0000000006190000.00000002.00000001.sdmp, ATuRNgegI7kl7Ua.exe, 00000000.00000003.215586670.00000000060AC000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.0000000006190000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.como	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244672949.00000000060A0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cno.	ATuRNgegI7kl7Ua.exe, 00000000.00000003.212561377.00000000060A3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	ATuRNgegI7kl7Ua.exe, 00000000.00000002.244730006.0000000006190000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/	ATuRNgegI7kl7Ua.exe, 00000000.00000003.214664649.00000000060D5000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
67.21.94.15	chefoowork.com	United States		46844	ST-BGPUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404156
Start date:	04.05.2021
Start time:	18:58:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ATuRNgegI7kl7Ua.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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@2/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.1%) • Quality average: 43.1% • Quality standard deviation: 38.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 168.61.161.212, 92.122.145.220, 104.43.139.144, 92.122.144.200, 20.82.210.154, 92.122.213.247, 92.122.213.194, 2.20.142.210, 2.20.142.209, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, store-images.s-microsoft.com-c.edgekey.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:59:53	API Interceptor	764x Sleep call for process: ATuRNgegI7kl7Ua.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
67.21.94.15	Vcv22W33OiwhO12.exe	Get hash	malicious	Browse	
	Catalog.exe	Get hash	malicious	Browse	
	5401628864_AWB_28002_2021-17-03 2.exe	Get hash	malicious	Browse	
	AVISO CREDITO PAGPROV.exe	Get hash	malicious	Browse	
	7070355.exe	Get hash	malicious	Browse	
	OC_402981675.exe	Get hash	malicious	Browse	
	OC_007943234.exe	Get hash	malicious	Browse	
	QIznD4DaCkKgV4J.exe	Get hash	malicious	Browse	
	U6ODBh62dJ0IYCK.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	OC_8403754263563.exe	Get hash	malicious	Browse	
	jc7xl20UOg.exe	Get hash	malicious	Browse	
	xlpnl7dBEb.exe	Get hash	malicious	Browse	
	rm1E9ZjuNd.exe	Get hash	malicious	Browse	
	DHL Shipment Info.exe	Get hash	malicious	Browse	
	RFQ.4414_122.exe	Get hash	malicious	Browse	
	GimRyEHi4ONqTEe.exe	Get hash	malicious	Browse	
	PO_2002837727_288772.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ST-BGPUS	Vcv22W33OiwhO12.exe	Get hash	malicious	Browse	• 67.21.94.15
	Catalog.exe	Get hash	malicious	Browse	• 67.21.94.15
	SecuriteInfo.com.Trojan.DownloaderNET.160.29545.exe	Get hash	malicious	Browse	• 67.21.94.4
	Proforma Invoice.xlsx	Get hash	malicious	Browse	• 204.188.203.155
	RCS76393.exe	Get hash	malicious	Browse	• 104.160.174.177
	eQLPRPErea.exe	Get hash	malicious	Browse	• 64.32.22.102
	UTcQK0heAfGWTLw.exe	Get hash	malicious	Browse	• 64.32.22.102
	RFQ # 1014397402856.pdf.exe	Get hash	malicious	Browse	• 204.188.203.155
	BIOTECHPO960488580.exe	Get hash	malicious	Browse	• 205.144.171.210
	GJK-KAOHSIUNG-2101.xlsx	Get hash	malicious	Browse	• 205.144.171.138
	New Purchase Order.exe	Get hash	malicious	Browse	• 204.188.203.155
	9311-32400.pdf.exe	Get hash	malicious	Browse	• 45.58.190.82
	ssyrNaO6AP.dll	Get hash	malicious	Browse	• 70.39.99.196
	5401628864_AWB_28002_2021-17-03 2.exe	Get hash	malicious	Browse	• 67.21.94.15
	SPmG3TLdax.exe	Get hash	malicious	Browse	• 204.188.203.155
	RDAW-180-47D.exe	Get hash	malicious	Browse	• 64.32.22.102
	Doc_3847468364836483638463,pdf.exe	Get hash	malicious	Browse	• 170.178.168.203
	gV8xdP8bas.exe	Get hash	malicious	Browse	• 104.160.174.169
	DHL.INFORMATION.TRACKING.exe	Get hash	malicious	Browse	• 67.21.94.4
	pVXFB33FzO.exe	Get hash	malicious	Browse	• 104.160.174.164

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ATuRNgegI7kl7Ua.exe.log

Process:	C:\Users\user\Desktop\ATuRNgegI7kl7Ua.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ATuRNgegI7kl7Ua.exe.log	
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
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):	7.643715367766411
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	ATuRNgegI7kl7Ua.exe
File size:	682496
MD5:	ec217acdf26636dd01ccba3dc7df5066
SHA1:	768c321ffe79e38f92682477a2b9b0e6122721ab
SHA256:	e27c7feb3112b0f8d3aa4195962fc2c430074179cbf6811874b49691c486e26f
SHA512:	e317158e54d3eb664fd4a9d8b79dc29f1d8c66d4213f311b31fcc37c575bcea5b0fb6674441f464360fdf7aadf337c199abaf4193a8cd63c5d90d2c76b3314c7
SSDEEP:	12288:Bngn6+vl0OKMw48B82j5RNDmCR6k1G9Dvv5eNvesqFYGjD+GtZV:Rgn/jOK348XTNR6kQ9qq3n
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..b.....F.... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a8046
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:	0x60910C13 [Tue May 4 08:55:47 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0

General

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa7ff4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xaa000	0x3e4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xac000	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	0xa604c	0xa6200	False	0.803329571106	data	7.65248683317	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xaa000	0x3e4	0x400	False	0.4169921875	data	3.16585068465	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xac000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xaa058	0x388	data		

Imports

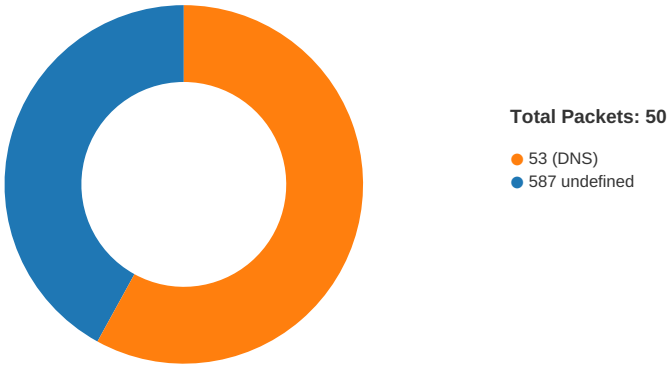
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Felix Jeyareuben 2012
Assembly Version	2.0.0.0
InternalName	WorkItem.exe
FileVersion	2.0
CompanyName	www.churchsw.org
LegalTrademarks	Church Software
Comments	
ProductName	Church Projector
ProductVersion	2.0
FileDescription	Church Projector
OriginalFilename	WorkItem.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:01:33.045916080 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:33.225610018 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:33.225836039 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:33.572180033 CEST	587	49742	67.21.94.15	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:01:33.574448109 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:33.754992962 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:33.755611897 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:33.938936949 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:33.987927914 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:33.992440939 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:34.183222055 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:34.183279991 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:34.183309078 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:34.183356047 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:34.183376074 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:34.183388948 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:34.183449030 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:34.188271046 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:34.220110893 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:34.400728941 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:34.456672907 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:34.471087933 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:34.651079893 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:34.654388905 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:34.837016106 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:34.837785006 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:35.036034107 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:35.037278891 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:35.217474937 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:35.218285084 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:35.434679985 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:35.435298920 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:35.615061045 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:35.619142056 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:35.619172096 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:35.619294882 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:35.619304895 CEST	49742	587	192.168.2.3	67.21.94.15
May 4, 2021 19:01:35.799060106 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:35.799082041 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:35.799091101 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:35.799104929 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:35.806989908 CEST	587	49742	67.21.94.15	192.168.2.3
May 4, 2021 19:01:35.847654104 CEST	49742	587	192.168.2.3	67.21.94.15

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:59:35.642340899 CEST	60152	53	192.168.2.3	8.8.8.8
May 4, 2021 18:59:35.691178083 CEST	53	60152	8.8.8.8	192.168.2.3
May 4, 2021 18:59:36.908426046 CEST	57544	53	192.168.2.3	8.8.8.8
May 4, 2021 18:59:36.957110882 CEST	53	57544	8.8.8.8	192.168.2.3
May 4, 2021 18:59:38.628599882 CEST	55984	53	192.168.2.3	8.8.8.8
May 4, 2021 18:59:38.691829920 CEST	53	55984	8.8.8.8	192.168.2.3
May 4, 2021 18:59:38.833957911 CEST	64185	53	192.168.2.3	8.8.8.8
May 4, 2021 18:59:38.885540962 CEST	53	64185	8.8.8.8	192.168.2.3
May 4, 2021 18:59:39.931950092 CEST	65110	53	192.168.2.3	8.8.8.8
May 4, 2021 18:59:39.983665943 CEST	53	65110	8.8.8.8	192.168.2.3
May 4, 2021 18:59:41.125822067 CEST	58361	53	192.168.2.3	8.8.8.8
May 4, 2021 18:59:41.177491903 CEST	53	58361	8.8.8.8	192.168.2.3
May 4, 2021 18:59:42.051585913 CEST	63492	53	192.168.2.3	8.8.8.8
May 4, 2021 18:59:42.100238085 CEST	53	63492	8.8.8.8	192.168.2.3
May 4, 2021 18:59:45.134418011 CEST	60831	53	192.168.2.3	8.8.8.8
May 4, 2021 18:59:45.183159113 CEST	53	60831	8.8.8.8	192.168.2.3
May 4, 2021 18:59:46.417371988 CEST	60100	53	192.168.2.3	8.8.8.8
May 4, 2021 18:59:46.468895912 CEST	53	60100	8.8.8.8	192.168.2.3
May 4, 2021 18:59:47.436151981 CEST	53195	53	192.168.2.3	8.8.8.8
May 4, 2021 18:59:47.484946012 CEST	53	53195	8.8.8.8	192.168.2.3
May 4, 2021 18:59:48.351166010 CEST	50141	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:59:48.402632952 CEST	53	50141	8.8.8.8	192.168.2.3
May 4, 2021 18:59:49.387048960 CEST	53023	53	192.168.2.3	8.8.8.8
May 4, 2021 18:59:49.435686111 CEST	53	53023	8.8.8.8	192.168.2.3
May 4, 2021 18:59:50.771469116 CEST	49563	53	192.168.2.3	8.8.8.8
May 4, 2021 18:59:50.823033094 CEST	53	49563	8.8.8.8	192.168.2.3
May 4, 2021 18:59:51.777339935 CEST	51352	53	192.168.2.3	8.8.8.8
May 4, 2021 18:59:51.829037905 CEST	53	51352	8.8.8.8	192.168.2.3
May 4, 2021 18:59:53.525948048 CEST	59349	53	192.168.2.3	8.8.8.8
May 4, 2021 18:59:53.574579000 CEST	53	59349	8.8.8.8	192.168.2.3
May 4, 2021 18:59:54.473582029 CEST	57084	53	192.168.2.3	8.8.8.8
May 4, 2021 18:59:54.522275925 CEST	53	57084	8.8.8.8	192.168.2.3
May 4, 2021 18:59:55.844422102 CEST	58823	53	192.168.2.3	8.8.8.8
May 4, 2021 18:59:55.894953012 CEST	53	58823	8.8.8.8	192.168.2.3
May 4, 2021 18:59:57.459867001 CEST	57568	53	192.168.2.3	8.8.8.8
May 4, 2021 18:59:57.508595943 CEST	53	57568	8.8.8.8	192.168.2.3
May 4, 2021 19:00:10.700999022 CEST	50540	53	192.168.2.3	8.8.8.8
May 4, 2021 19:00:10.759893894 CEST	53	50540	8.8.8.8	192.168.2.3
May 4, 2021 19:00:13.654460907 CEST	54366	53	192.168.2.3	8.8.8.8
May 4, 2021 19:00:13.703332901 CEST	53	54366	8.8.8.8	192.168.2.3
May 4, 2021 19:00:30.110204935 CEST	53034	53	192.168.2.3	8.8.8.8
May 4, 2021 19:00:30.172071934 CEST	53	53034	8.8.8.8	192.168.2.3
May 4, 2021 19:00:30.997025967 CEST	57762	53	192.168.2.3	8.8.8.8
May 4, 2021 19:00:31.059205055 CEST	53	57762	8.8.8.8	192.168.2.3
May 4, 2021 19:00:43.876801968 CEST	55435	53	192.168.2.3	8.8.8.8
May 4, 2021 19:00:43.942065954 CEST	53	55435	8.8.8.8	192.168.2.3
May 4, 2021 19:00:53.329466105 CEST	50713	53	192.168.2.3	8.8.8.8
May 4, 2021 19:00:53.378694057 CEST	53	50713	8.8.8.8	192.168.2.3
May 4, 2021 19:00:58.233031034 CEST	56132	53	192.168.2.3	8.8.8.8
May 4, 2021 19:00:58.294730902 CEST	53	56132	8.8.8.8	192.168.2.3
May 4, 2021 19:01:29.667176962 CEST	58987	53	192.168.2.3	8.8.8.8
May 4, 2021 19:01:29.715739012 CEST	53	58987	8.8.8.8	192.168.2.3
May 4, 2021 19:01:32.450627089 CEST	56579	53	192.168.2.3	8.8.8.8
May 4, 2021 19:01:32.523022890 CEST	53	56579	8.8.8.8	192.168.2.3
May 4, 2021 19:01:32.583157063 CEST	60633	53	192.168.2.3	8.8.8.8
May 4, 2021 19:01:32.799722910 CEST	53	60633	8.8.8.8	192.168.2.3
May 4, 2021 19:01:32.819849014 CEST	61292	53	192.168.2.3	8.8.8.8
May 4, 2021 19:01:33.031466007 CEST	53	61292	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 19:01:32.583157063 CEST	192.168.2.3	8.8.8.8	0xdcaa	Standard query (0)	mail.chefoowork.com	A (IP address)	IN (0x0001)
May 4, 2021 19:01:32.819849014 CEST	192.168.2.3	8.8.8.8	0xf644	Standard query (0)	mail.chefoowork.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 19:01:32.799722910 CEST	8.8.8.8	192.168.2.3	0xdcaa	No error (0)	mail.chefoowork.com	chefoowork.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:01:32.799722910 CEST	8.8.8.8	192.168.2.3	0xdcaa	No error (0)	chefoowork.com		67.21.94.15	A (IP address)	IN (0x0001)
May 4, 2021 19:01:33.031466007 CEST	8.8.8.8	192.168.2.3	0xf644	No error (0)	mail.chefoowork.com	chefoowork.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 19:01:33.031466007 CEST	8.8.8.8	192.168.2.3	0xf644	No error (0)	chefoowork.com		67.21.94.15	A (IP address)	IN (0x0001)

SMTP Packets

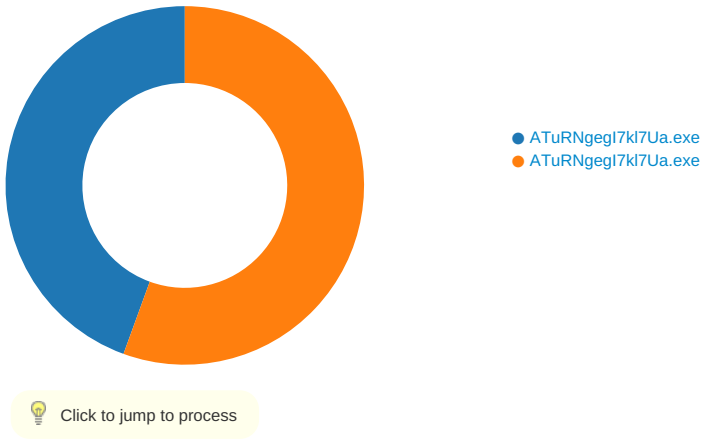
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 4, 2021 19:01:33.572180033 CEST	587	49742	67.21.94.15	192.168.2.3	220-web2.changeip.com ESMTP Exim 4.94 #2 Tue, 04 May 2021 13:01:32 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 4, 2021 19:01:33.574448109 CEST	49742	587	192.168.2.3	67.21.94.15	EHLO 128757
May 4, 2021 19:01:33.754992962 CEST	587	49742	67.21.94.15	192.168.2.3	250-web2.changeip.com Hello 128757 [84.17.52.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-STARTTLS 250 HELP
May 4, 2021 19:01:33.755611897 CEST	49742	587	192.168.2.3	67.21.94.15	STARTTLS
May 4, 2021 19:01:33.938936949 CEST	587	49742	67.21.94.15	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: ATuRNgegI7kl7Ua.exe PID: 5856 Parent PID: 5620

General

Start time:	18:59:42
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\ATuRNgegI7kl7Ua.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ATuRNgegI7kl7Ua.exe'
Imagebase:	0xb80000
File size:	682496 bytes
MD5 hash:	EC217ACDF26636DD01CCBA3DC7DF5066
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: 00000000.00000002.239732017.0000000003F39000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.235727199.0000000002FAC000.00000004.00000001.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	6DEECF06	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	6DEECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ATuRNgegI7kl7Ua.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1FC78D	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\ATuRNgegI7kl7Ua.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	6E1FC907	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	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile

Analysis Process: ATuRNgegI7kl7Ua.exe PID: 1368 Parent PID: 5856

General

Start time:	18:59:55
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\ATuRNgegI7kl7Ua.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\ATuRNgegI7kl7Ua.exe
Imagebase:	0xa50000
File size:	682496 bytes
MD5 hash:	EC217ACDF26636DD01CCBA3DC7DF5066
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.480281925.0000000002E11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.480281925.0000000002E11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.475257684.0000000000402000.00000040.00000001.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	6DEECF06	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	6DEECF06	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	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile

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	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CD31B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\1e0fb828-c11d-4329-9d11-24495fc46ca7	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6CD31B4F	ReadFile

Disassembly

Code Analysis