ID: 652383
Sample Name:
oAE7nqtsNA.exe
Cookbook: default.jbs
Time: 09:31:10
Date: 26/06/2022
Version: 35.0.0 Citrine

Table of Contents

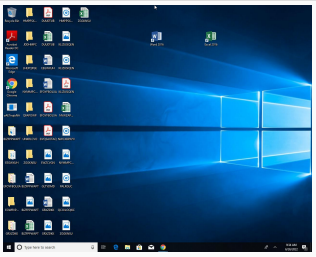
Windows Analysis Report

oAE7nqtsNA.exe

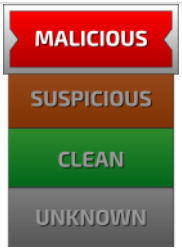
Overview

General Information

Sample Name:	oAE7nqtsNA.exe
Analysis ID:	652383
MD5:	0f20f2a0d366d09.
SHA1:	e838dc5484de4f..
SHA256:	c5d4a26f1de900..
Tags:	exe SnakeKeylogger
Infos:	



Detection



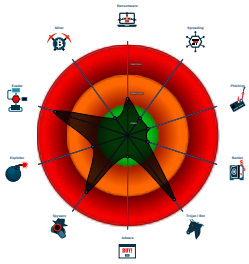
Snake Keylogger

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Snake Keylogger
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Yara detected AntiVM3
- Antivirus / Scanner detection for sub…
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal ftp login c…
- .NET source code references suspic…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- May check the online IP address of…

Classification



Process Tree

- **System is w10x64**
- oAE7nqtsNA.exe (PID: 7108 cmdline: "C:\Users\user\Desktop\oAE7nqtsNA.exe" MD5: 0F20F2A0D366D09D7F9775220F024638)
  - oAE7nqtsNA.exe (PID: 6516 cmdline: C:\Users\user\Desktop\oAE7nqtsNA.exe MD5: 0F20F2A0D366D09D7F9775220F024638)
- **cleanup**

Malware Configuration

Threatname: Snake Keylogger


```
{
  "Exfil Mode": "SMTP",
  "Username": "frankjoelog@valete.buzz",
  "Password": "7213575aceACE@#$",
  "Host": "cp5ua.hyperhost.ua",
  "Port": "frankjoe@valete.buzz"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.417015473.000000000331A000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000000.410485061.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
00000005.00000000.410485061.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000000.410485061.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000005.00000000.410485061.0000000000402000.00000040.00000400.00020000.00000000.sdmp	MALWARE_Win_SnakeKeylogger	Detects Snake Keylogger	ditekSHen	• 0x17418:$x1: $%SMTPDV$ • 0x1742e:$x2: $#TheHashHere%& • 0x187c8:$x3: %FTPDV$ • 0x18890:$x4: $%TelegramDv$ • 0x14d34:$x5: KeyLoggerEventArgs • 0x150ca:$x5: KeyLoggerEventArgs • 0x18838:$m1: \| Snake Keylogger • 0x188f0:$m1: | Snake Keylogger • 0x18a44:$m1: \| Snake Keylogger • 0x18b6a:$m1: | Snake Keylogger • 0x18cc4:$m1: \| Snake Keylogger • 0x187ec:$m2: Clipboard Logs ID • 0x189fa:$m2: Screenshot Logs ID • 0x18b0e:$m2: keystroke Logs ID • 0x18cfa:$m3: SnakePW • 0x189d2:$m4: \SnakeKeylogger\
Click to see the 27 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.oAE7nqtsNA.exe.4e715a0.9.raw.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x1b35e:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x3af7e:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x5a99e:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x1a547:$a3: \Google\Chrome\User Data\Default\Login Data • 0x3a167:$a3: \Google\Chrome\User Data\Default\Login Data • 0x59b87:$a3: \Google\Chrome\User Data\Default\Login Data • 0x1a98e:$a4: \Orbitum\User Data\Default\Login Data • 0x3a5ae:$a4: \Orbitum\User Data\Default\Login Data • 0x59fce:$a4: \Orbitum\User Data\Default\Login Data • 0x1bb0f:$a5: \Kometa\User Data\Default\Login Data • 0x3b72f:$a5: \Kometa\User Data\Default\Login Data • 0x5b14f:$a5: \Kometa\User Data\Default\Login Data
0.2.oAE7nqtsNA.exe.4e715a0.9.raw.unpack	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
0.2.oAE7nqtsNA.exe.4e715a0.9.raw.unpack	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
0.2.oAE7nqtsNA.exe.4e715a0.9.raw.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
0.2.oAE7nqtsNA.exe.4e715a0.9.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 73 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Networking

May check the online IP address of the machine

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Snake Keylogger

Yara detected Telegram RAT

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality

Yara detected Snake Keylogger

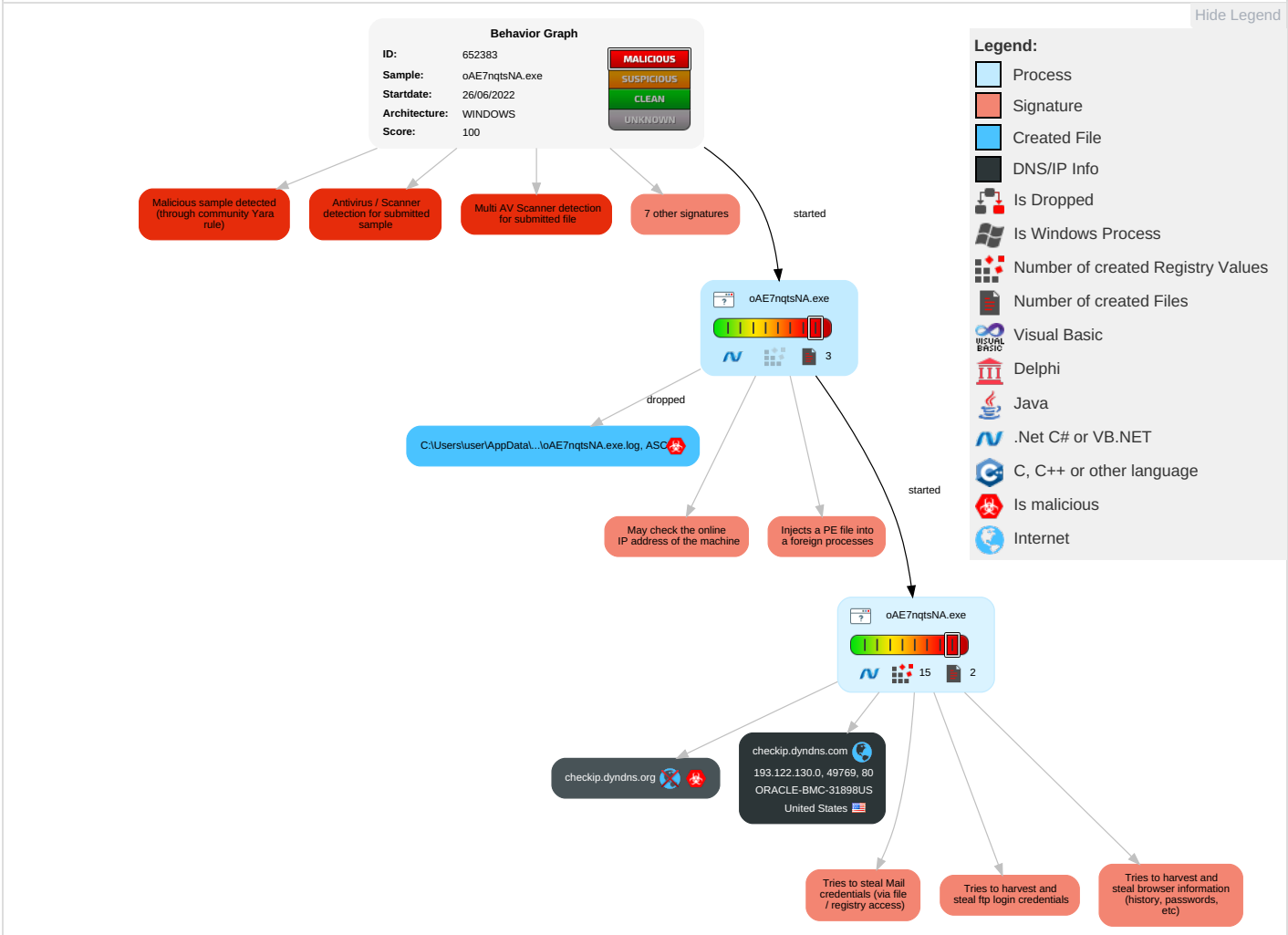
Yara detected Telegram RAT

Mitre Att&ck Matrix

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

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

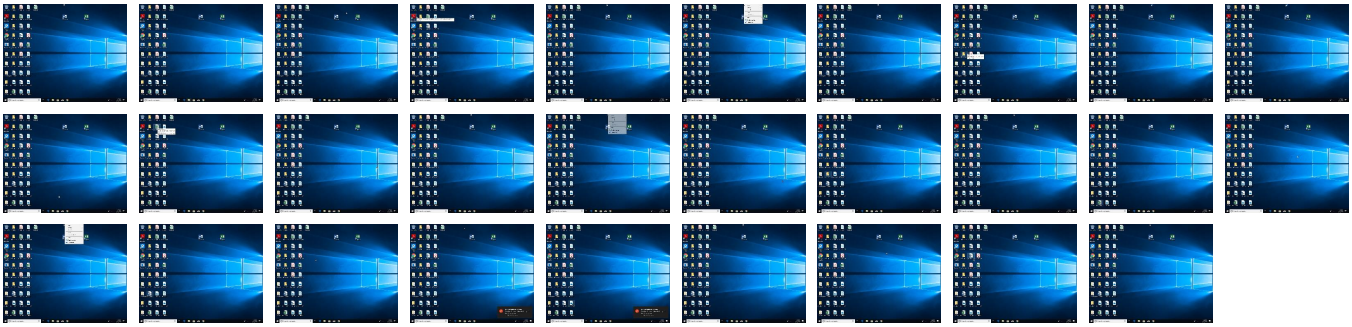
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
oAE7nqtsNA.exe	37%	Virustotal		Browse
oAE7nqtsNA.exe	62%	ReversingLabs	ByteCode-MSIL.Spyware.SnakeLogger	

Source	Detection	Scanner	Label	Link
oAE7nqtsNA.exe	100%	Avira	HEUR/AGEN.1202539	
oAE7nqtsNA.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.oAE7nqtsNA.exe.400000.4.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
5.0.oAE7nqtsNA.exe.400000.8.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
5.0.oAE7nqtsNA.exe.e60000.0.unpack	100%	Avira	HEUR/AGEN.1202539		Download File
5.2.oAE7nqtsNA.exe.e60000.1.unpack	100%	Avira	HEUR/AGEN.1202539		Download File
5.0.oAE7nqtsNA.exe.e60000.9.unpack	100%	Avira	HEUR/AGEN.1202539		Download File
5.0.oAE7nqtsNA.exe.400000.6.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
5.0.oAE7nqtsNA.exe.e60000.7.unpack	100%	Avira	HEUR/AGEN.1202539		Download File
5.2.oAE7nqtsNA.exe.400000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
5.0.oAE7nqtsNA.exe.e60000.3.unpack	100%	Avira	HEUR/AGEN.1202539		Download File
5.0.oAE7nqtsNA.exe.e60000.13.unpack	100%	Avira	HEUR/AGEN.1202539		Download File
5.0.oAE7nqtsNA.exe.e60000.5.unpack	100%	Avira	HEUR/AGEN.1202539		Download File
5.0.oAE7nqtsNA.exe.400000.12.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
5.0.oAE7nqtsNA.exe.400000.10.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
5.0.oAE7nqtsNA.exe.e60000.11.unpack	100%	Avira	HEUR/AGEN.1202539		Download File
5.0.oAE7nqtsNA.exe.e60000.1.unpack	100%	Avira	HEUR/AGEN.1202539		Download File
0.2.oAE7nqtsNA.exe.e30000.0.unpack	100%	Avira	HEUR/AGEN.1202539		Download File
0.0.oAE7nqtsNA.exe.e30000.0.unpack	100%	Avira	HEUR/AGEN.1202539		Download File
5.0.oAE7nqtsNA.exe.e60000.2.unpack	100%	Avira	HEUR/AGEN.1202539		Download File

Domains

Source	Detection	Scanner	Label	Link
checkip.dyndns.com	0%	Virustotal		Browse
checkip.dyndns.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.tiro.comnt	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comcom2:	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.monotype.u5Ifm	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://checkip.dyndns.org4	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://checkip.dyndns.org/	0%	URL Reputation	safe	
http://www.carterandcone.com8	0%	URL Reputation	safe	
http://checkip.dyndns.org/q	0%	URL Reputation	safe	
http://www.carterandcone.comCm	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://checkip.dyndns.com	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/j	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.urwpp.deQ?og	0%	Avira URL Cloud	safe	
http://www.urwpp.deet	0%	Avira URL Cloud	safe	
http://www.fontbureau.comaA	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org	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.tiro.comu?sg	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.urwpp.deoM?	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.urwpp.der	0%	URL Reputation	safe	
http://www.urwpp.deM?	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
checkip.dyndns.com	193.122.130.0	true	false	• 0%, Virustotal, Browse	unknown
checkip.dyndns.org	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/	false	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.comnt	oAE7nqtsNA.exe, 00000000.00000003.373562364.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

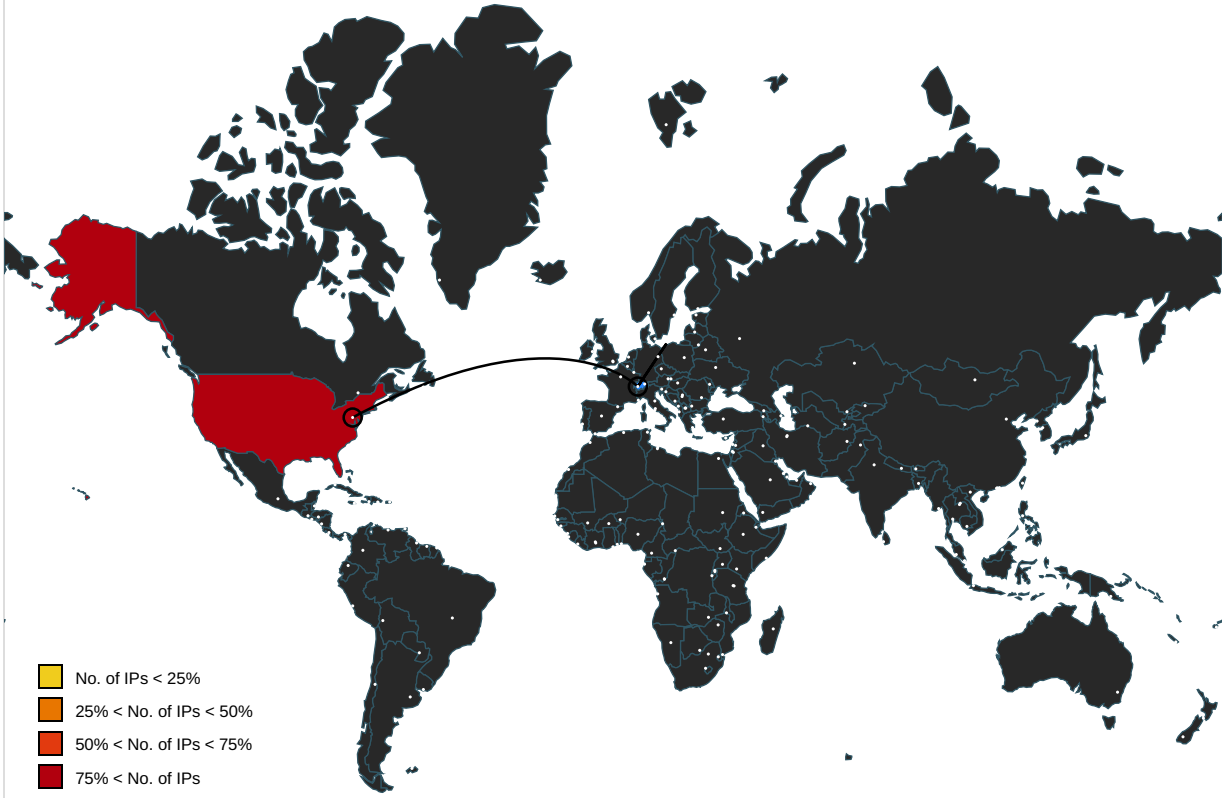
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot	oAE7nqtsNA.exe, 00000000.00000002.419701815.0000000004E4F000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000005.00000000.410485061.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comcom2:	oAE7nqtsNA.exe, 00000000.00000003.373501516.0000000008602000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.373488583.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	oAE7nqtsNA.exe, 00000000.00000003.373562364.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.372804822.00000000085E0000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.372643733.00000000085D5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	oAE7nqtsNA.exe, 00000000.00000003.378280858.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	oAE7nqtsNA.exe, 00000000.00000003.373501516.0000000008602000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.373406882.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.373488583.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.monotype.u5lfm	oAE7nqtsNA.exe, 00000000.00000003.385023609.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.385142286.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.385086768.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	oAE7nqtsNA.exe, 00000000.00000003.370199665.00000000085D2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.org4	oAE7nqtsNA.exe, 00000005.00000002.633579868.0000000003221000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgrita	oAE7nqtsNA.exe, 00000000.00000003.414103381.00000000085D0000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000002.422768964.00000000085D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com8	oAE7nqtsNA.exe, 00000000.00000003.373501516.0000000008602000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.373488583.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.org/q	oAE7nqtsNA.exe, 00000000.00000002.419701815.0000000004E4F000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000005.00000000.410485061.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comCm	oAE7nqtsNA.exe, 00000000.00000003.373501516.0000000008602000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.373488583.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.com	oAE7nqtsNA.exe, 00000005.00000002.633758054.00000000032C7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	oAE7nqtsNA.exe, 00000000.00000003.377510752.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.377635947.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.377735120.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.377558699.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	oAE7nqtsNA.exe, 00000005.00000002.633579868.0000000003221000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersp	oAE7nqtsNA.exe, 00000000.00000003.377820878.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.377871680.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	oAE7nqtsNA.exe, 00000000.00000003.375462201.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.375487989.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.375434034.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.375524462.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.375549410.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersr	oAE7nqtsNA.exe, 00000000.00000003.379545847.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.379660966.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.379475463.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.379618788.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.379413748.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/j	oAE7nqtsNA.exe, 00000000.00000003.382093813.000000000860F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/	oAE7nqtsNA.exe, 00000000.00000003.382093813.000000000860F000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.382162334.000000000860F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comn	oAE7nqtsNA.exe, 00000000.00000003.372643733.00000000085D5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deQ?og	oAE7nqtsNA.exe, 00000000.00000003.380334792.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.380092149.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.380247772.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.380002455.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deet	oAE7nqtsNA.exe, 00000000.00000003.377510752.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.377635947.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.377735120.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.377558699.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.377783630.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comaA	oAE7nqtsNA.exe, 00000000.00000003.414103381.00000000085D0000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000002.422768964.00000000085D0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://checkip.dyndns.org	oAE7nqtsNA.exe, 00000005.00000002.633579868.0000000003221000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000005.00000002.633758054.00000000032C7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	oAE7nqtsNA.exe, 00000000.00000003.372589089.00000000085DF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.378710748.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers$4	oAE7nqtsNA.exe, 00000000.00000003.386273147.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.comu?sg	oAE7nqtsNA.exe, 00000000.00000003.373562364.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.	oAE7nqtsNA.exe, 00000000.00000003.386180535.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.386020175.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deoM?	oAE7nqtsNA.exe, 00000000.00000003.380002455.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.der	oAE7nqtsNA.exe, 00000000.00000003.380092149.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.380247772.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.380002455.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deM?	oAE7nqtsNA.exe, 00000000.00000003.377510752.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.377635947.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.377735120.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.377558699.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.377783630.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	oAE7nqtsNA.exe, 00000000.00000002.423042498.0000000009862000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.378710748.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers94	oAE7nqtsNA.exe, 00000000.00000003.379329452.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.379475463.00000000085FE000.00000004.00000800.00020000.00000000.sdmp, oAE7nqtsNA.exe, 00000000.00000003.379413748.00000000085FE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://picsum.photos/80	oAE7nqtsNA.exe	false		high
http://www.fontbureau.com/designers/	oAE7nqtsNA.exe, 00000000.00000003.377796525.000000000860F000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.122.130.0	checkip.dyndns.com	United States		31898	ORACLE-BMC-31898US	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	652383
Start date and time: 26/06/202209:31:10	2022-06-26 09:31:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	oAE7nqtsNA.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:	19
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:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.2%) • Quality average: 50.9% • Quality standard deviation: 43.7%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:32:33	API Interceptor	1x Sleep call for process: oAE7nqtsNA.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\oAE7nqtsNA.exe.log

Process:	C:\Users\user\Desktop\oAE7nqtsNA.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8910721031299795
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:	oAE7nqtsNA.exe
File size:	539136
MD5:	0f20f2a0d366d09d7f9775220f024638
SHA1:	e838dc5484de4f2bc6d43290e8e2e860f32182de
SHA256:	c5d4a26f1de9008689bf4ecf2eebd6c860282f32db70d982f5281c4630fb4cac
SHA512:	dea80ff93a97c82cc8d8e84e1cb3ccc7bec651d1fe30d168c8fb466ec1e15647f11ff14fffeabf269a1b80f1610df28355dbbb5494585455757fd8963d47061e

SSDEEP:	12288:hDK3rT/keuQ94+66h1FNHXOEo0ItTvbs8FK05gY/:hDKbnhh1FFOEetPs8
TLSH:	04B4D09D322472EFC857D076DEA82C78AB60347B531B8213941325EE9A5DA97CF214F3
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...t.U...............0..2...........Q... ...`....@.. ....@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x48511e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xD255CC74 [Tue Oct 28 00:51:00 2081 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x850cc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x86000	0x398	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	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	0x83124	0x83200	False	0.920081997735939	data	7.8977969416018095	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x86000	0x398	0x400	False	0.37890625	data	2.9056920095509953	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

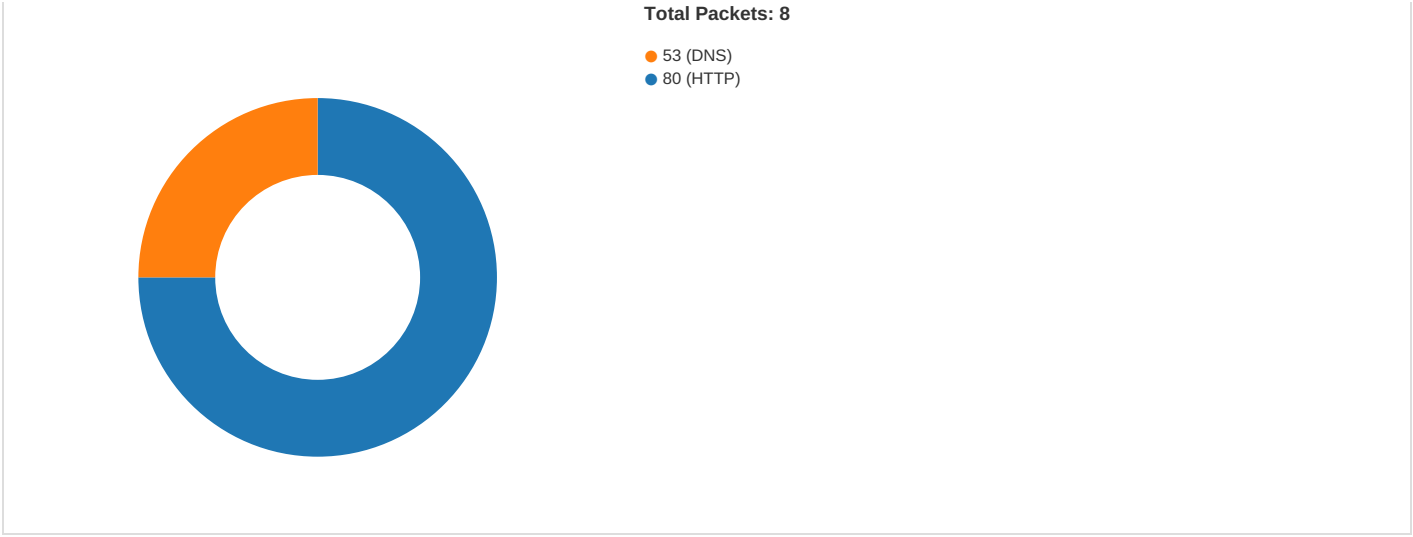
Name	RVA	Size	Type	Language	Country
RT_VERSION	0x86058	0x33c	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:32:49.748342991 CEST	49769	80	192.168.2.6	193.122.130.0
Jun 26, 2022 09:32:49.860111952 CEST	80	49769	193.122.130.0	192.168.2.6
Jun 26, 2022 09:32:49.861855030 CEST	49769	80	192.168.2.6	193.122.130.0
Jun 26, 2022 09:32:49.865596056 CEST	49769	80	192.168.2.6	193.122.130.0
Jun 26, 2022 09:32:49.977227926 CEST	80	49769	193.122.130.0	192.168.2.6
Jun 26, 2022 09:32:49.977797985 CEST	80	49769	193.122.130.0	192.168.2.6
Jun 26, 2022 09:32:50.085800886 CEST	49769	80	192.168.2.6	193.122.130.0
Jun 26, 2022 09:33:54.977902889 CEST	80	49769	193.122.130.0	192.168.2.6
Jun 26, 2022 09:33:54.981185913 CEST	49769	80	192.168.2.6	193.122.130.0
Jun 26, 2022 09:34:30.021599054 CEST	49769	80	192.168.2.6	193.122.130.0
Jun 26, 2022 09:34:30.133021116 CEST	80	49769	193.122.130.0	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:32:49.640799046 CEST	51748	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:32:49.662122011 CEST	53	51748	8.8.8.8	192.168.2.6
Jun 26, 2022 09:32:49.690249920 CEST	61116	53	192.168.2.6	8.8.8.8
Jun 26, 2022 09:32:49.711349010 CEST	53	61116	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 26, 2022 09:32:49.640799046 CEST	192.168.2.6	8.8.8.8	0x372b	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Jun 26, 2022 09:32:49.690249920 CEST	192.168.2.6	8.8.8.8	0x7319	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 26, 2022 09:32:49.662122011 CEST	8.8.8.8	192.168.2.6	0x372b	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Jun 26, 2022 09:32:49.662122011 CEST	8.8.8.8	192.168.2.6	0x372b	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)
Jun 26, 2022 09:32:49.662122011 CEST	8.8.8.8	192.168.2.6	0x372b	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)
Jun 26, 2022 09:32:49.662122011 CEST	8.8.8.8	192.168.2.6	0x372b	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)
Jun 26, 2022 09:32:49.662122011 CEST	8.8.8.8	192.168.2.6	0x372b	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)
Jun 26, 2022 09:32:49.662122011 CEST	8.8.8.8	192.168.2.6	0x372b	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 26, 2022 09:32:49.711349010 CEST	8.8.8.8	192.168.2.6	0x7319	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Jun 26, 2022 09:32:49.711349010 CEST	8.8.8.8	192.168.2.6	0x7319	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)
Jun 26, 2022 09:32:49.711349010 CEST	8.8.8.8	192.168.2.6	0x7319	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)
Jun 26, 2022 09:32:49.711349010 CEST	8.8.8.8	192.168.2.6	0x7319	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)
Jun 26, 2022 09:32:49.711349010 CEST	8.8.8.8	192.168.2.6	0x7319	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)
Jun 26, 2022 09:32:49.711349010 CEST	8.8.8.8	192.168.2.6	0x7319	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- checkip.dyndns.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49769	193.122.130.0	80	C:\Users\user\Desktop\oAE7nqtsNA.exe

Timestamp	kBytes transferred	Direction	Data
Jun 26, 2022 09:32:49.865596056 CEST	1086	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org Connection: Keep-Alive
Jun 26, 2022 09:32:49.977797985 CEST	1086	IN	HTTP/1.1 200 OK Date: Sun, 26 Jun 2022 07:32:49 GMT Content-Type: text/html Content-Length: 106 Connection: keep-alive Cache-Control: no-cache Pragma: no-cache Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 31 30 32 2e 31 32 39 2e 31 34 33 2e 36 31 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 102.129.143.61</body></html>

Statistics

Behavior

System Behavior

Analysis Process: oAE7nqtsNA.exe PID: **7108**, Parent PID: **2124**

General

Target ID:	0
Start time:	09:32:19
Start date:	26/06/2022
Path:	C:\Users\user\Desktop\oAE7nqtsNA.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\oAE7nqtsNA.exe"
Imagebase:	0xe30000
File size:	539136 bytes
MD5 hash:	0F20F2A0D366D09D7F9775220F024638
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.417015473.000000000331A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.419701815.0000000004E4F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000002.419701815.0000000004E4F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.419701815.0000000004E4F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000002.419701815.0000000004E4F000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
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	6D92CF06	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	6D92CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\oAE7nqtsNA.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DC3C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\oAE7nqtsNA.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DC3C907	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	6D905705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D905705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D90CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D905705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D905705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C771B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C771B4F	ReadFile

Analysis Process: oAE7nqtsNA.exe PID: **6516**, Parent PID: **7108**

General

Target ID:	5
Start time:	09:32:40
Start date:	26/06/2022
Path:	C:\Users\user\Desktop\oAE7nqtsNA.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\oAE7nqtsNA.exe
Imagebase:	0xe60000
File size:	539136 bytes
MD5 hash:	0F20F2A0D366D09D7F9775220F024638
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000005.00000000.410485061.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000005.00000000.410485061.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000000.410485061.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000005.00000000.410485061.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000005.00000002.632442217.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000005.00000002.632442217.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.632442217.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000005.00000002.632442217.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000005.00000000.411281858.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000005.00000000.411281858.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000000.411281858.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000005.00000000.411281858.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000005.00000000.410840955.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000005.00000000.410840955.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000000.410840955.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000005.00000000.410840955.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000005.00000000.411712452.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000005.00000000.411712452.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000000.411712452.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000005.00000000.411712452.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen
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	6D92CF06	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	6D92CF06	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	6D905705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D905705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D90CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D905705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D905705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C771B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C771B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C771B4F	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly