



ID: 756297
Sample Name: file.exe
Cookbook: default.jbs
Time: 00:10:13
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report file.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Snake Keylogger 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 6
System Summary 6
Data Obfuscation 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 14
Public IPs 15
Private 15
General Information 15
Warnings 16
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASNs 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\file.exe.log 16
Static File Info 17
General 17
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 17
Data Directories 19
Sections 20
Resources 20
Imports 20
Network Behavior 20
Snort IDS Alerts 20
Network Port Distribution 20
TCP Packets 20
UDP Packets 21
DNS Queries 21
DNS Answers 21
HTTP Request Dependency Graph 21

Statistics 22
Behavior 22
System Behavior 22
Analysis Process: file.exePID: 1128, Parent PID: 3528 22
General 22
File Activities 22
File Created 22
File Written 23
File Read 23
Analysis Process: file.exePID: 5916, Parent PID: 1128 23
General 24
Analysis Process: file.exePID: 4844, Parent PID: 1128 24
General 24
Analysis Process: file.exePID: 5260, Parent PID: 1128 24
General 24
File Activities 25
File Created 25
File Read 25
Registry Activities 25
Analysis Process: audiodg.exePID: 4844, Parent PID: 1596 25
General 25
Disassembly 26

Copyright Joe Security LLC 2022

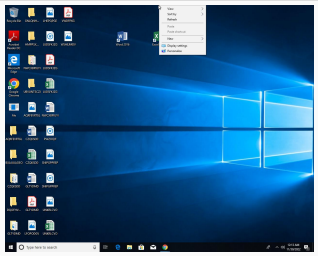
Windows Analysis Report

file.exe

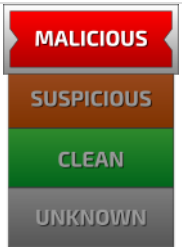
Overview

General Information

Sample Name:	file.exe
Analysis ID:	756297
MD5:	cfc1c66cba07da…
SHA1:	10451947894a7a..
SHA256:	addc1564d69b11..
Tags:	NET exe MSIL SnakeKeylogger
Infos:	



Detection



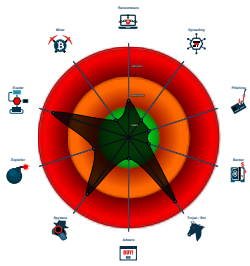
Snake Keylogger

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…
- Snort IDS alert for network traffic
- 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…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 1128 cmdline: C:\Users\user\Desktop\file.exe MD5: CFC1C66CBA07DAEF1E8AC13D5E042E7A)
  - file.exe (PID: 5916 cmdline: C:\Users\user\Desktop\file.exe MD5: CFC1C66CBA07DAEF1E8AC13D5E042E7A)
  - file.exe (PID: 4844 cmdline: C:\Users\user\Desktop\file.exe MD5: CFC1C66CBA07DAEF1E8AC13D5E042E7A)
  - file.exe (PID: 5260 cmdline: C:\Users\user\Desktop\file.exe MD5: CFC1C66CBA07DAEF1E8AC13D5E042E7A)
  - audiodg.exe (PID: 4844 cmdline: C:\Windows\system32\AUDIODG.EXE 0x364 MD5: 0B245353F92DF527AA7613BA2C0DA023)
- **cleanup**

Malware Configuration

Threatname: Snake Keylogger

```
{
  "Exfil Mode": "SMTP",
  "Username": "arinzelog@saonline.xyz",
  "Password": "7213575aceACE@#$",
  "Host": "cp5ua.hyperhost.ua",
  "Port": "587"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.365680487.0000000003439000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.367556703.0000000004135000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000000.00000002.367556703.0000000004135000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
00000000.00000002.367556703.0000000004135000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.367556703.0000000004135000.00000004.00000800.00020000.00000000.sdmp	MALWARE_Win_SnakeKeylogger	Detects Snake Keylogger	ditekSHen	• 0x522dc:$x1: $%SMTPDV$ • 0x522f2:$x2: $#TheHashHere%& • 0x537f3:$x3: %FTPDV$ • 0x538b7:$x4: $%TelegramDv$ • 0x4fb75:$x5: KeyLoggerEventArgs • 0x4ff0b:$x5: KeyLoggerEventArgs • 0x53817:$m2: Clipboard Logs ID • 0x53a1d:$m2: Screenshot Logs ID • 0x53b2d:$m2: keystroke Logs ID • 0x53d11:$m3: SnakePW • 0x539f5:$m4: \SnakeKeylogger\
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.file.exe.416fa10.6.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x198d3:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x18b05:$a3: \Google\Chrome\User Data\Default\Login Data • 0x18f38:$a4: \Orbitum\User Data\Default\Login Data • 0x1a05f:$a5: \Kometa\User Data\Default\Login Data
0.2.file.exe.416fa10.6.unpack	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
0.2.file.exe.416fa10.6.unpack	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
0.2.file.exe.416fa10.6.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0.2.file.exe.416fa10.6.unpack	INDICATOR_SUSPICIOUS_EXE_DotNetProcHook	Detects executables with potential process hoocking	ditekSHen	• 0x12d07:$s1: UnHook • 0x12d0e:$s2: SetHook • 0x12d16:$s3: CallNextHook • 0x12d23:$s4: _hook
Click to see the 33 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN 404/Snake/Matiex Keylogger Style External IP Check - Source IP: 192.168.2.4 - Destination IP: 193.122.130.0

Timestamp:	192.168.2.4193.122.130.049696802039190 11/30/22-00:11:36.516564
SID:	2039190
Source Port:	49696
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Networking



Snort IDS alert for network traffic

May check the online IP address of the machine

Yara detected Generic Downloader

System Summary



Malicious sample detected (through community Yara rule)

Data Obfuscation



.NET source code contains potential unpacker

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

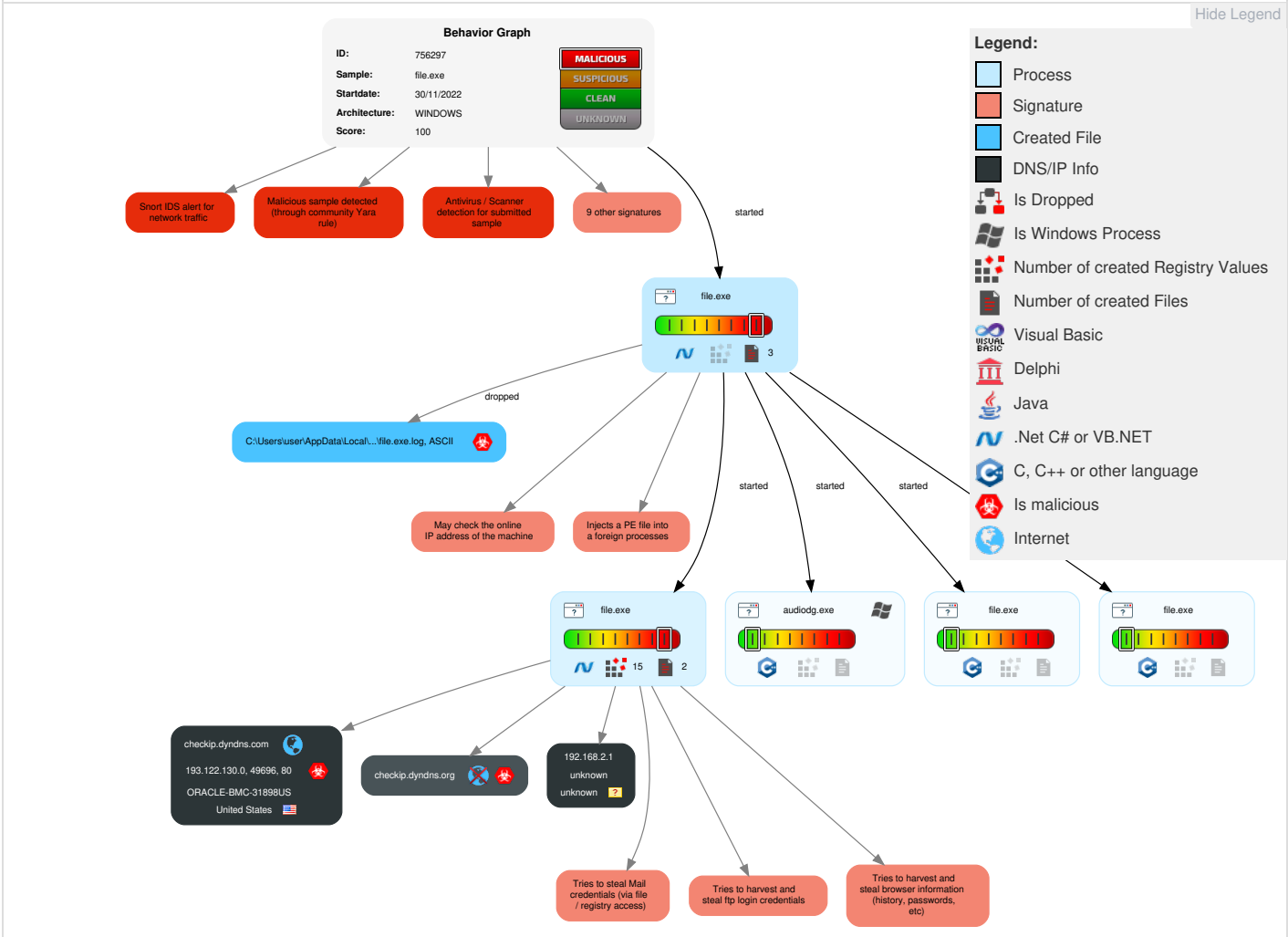
Mitre Att&ck Matrix

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)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 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

Copyright Joe Security LLC 2022

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	3 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	1 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
file.exe	38%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	
file.exe	25%	Virustotal		Browse
file.exe	100%	Avira	HEUR/AGEN.1249296	
file.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.file.exe.400000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
0.0.file.exe.aa0000.0.unpack	100%	Avira	HEUR/AGEN.1249296		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	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.sajatypeworks.com	0%	URL Reputation	safe	
http://checkip.dyndns.org4	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://checkip.dyndns.org/	0%	URL Reputation	safe	
http://checkip.dyndns.org/q	0%	URL Reputation	safe	
http://www.urwpp.de2	0%	URL Reputation	safe	
http://www.founder.com.cn/cn_	0%	URL Reputation	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.urwpp.dewa	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.tiro.com#	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://checkip.dyndns.org	0%	URL Reputation	safe	
http://www.carterandcone.comt	0%	URL Reputation	safe	
http://www.zhongyicts.com.cne	0%	URL Reputation	safe	
http://en.w	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.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn9)z	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnn-uAofz	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnmd	0%	Avira URL Cloud	safe	
http://www.carterandcone.comuctP	0%	Avira URL Cloud	safe	
http://www.urwpp.dew	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2022

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
checkip.dyndns.com	193.122.130.0	true	true		unknown
checkip.dyndns.org	unknown	unknown	true		unknown

Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	file.exe, 00000000.00000002.372638789.000000006FE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	file.exe, 00000000.00000002.372638789.000000006FE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	file.exe, 00000000.00000002.372638789.000000006FE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot	file.exe, 00000000.00000002.367556703.000000004135000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.370182647.000000000445D000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000003.00000000.356501796.00000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cnmd	file.exe, 00000000.00000003.323222872.000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323273225.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323456584.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.322784264.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.322849771.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.322819666.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323165080.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323364666.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	file.exe, 00000000.00000002.372638789.000000006FE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html8	file.exe, 00000000.00000003.328017976.000000005DED000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.327948700.0000000005DED000.00000004.00000800.00020000.00000000.sdmp	false		high

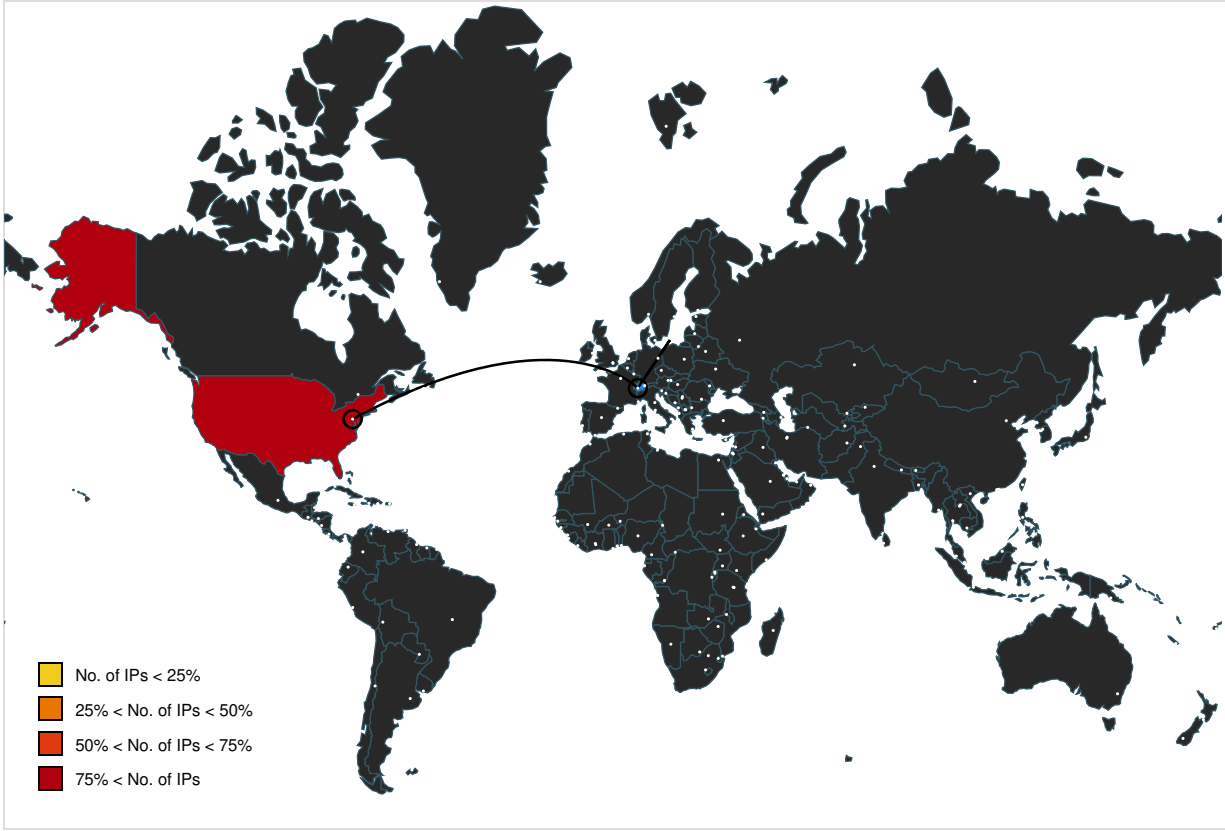
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com	file.exe, 00000000.00000002.372638789.00 00000006FE2000.00000004.00000800.0002000 0.00000000.sdmp, file.exe, 00000000.0000 0003.323570476.0000000005E1E000.00000004 .00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323578756.00000000 05E1F000.00000004.00000800.00020000.0000 0000.sdmp, file.exe, 00000000.00000003.3 22410540.0000000005E1E000.00000004.00000 800.00020000.00000000.sdmp, file.exe, 00 000000.00000003.323642134.0000000005E1F0 00.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.322390325.0000000 005E1E000.00000004.00000800.00020000.000 00000.sdmp, file.exe, 00000000.00000003. 323539855.0000000005E1E000.00000004.0000 0800.00020000.00000000.sdmp, file.exe, 0 0000000.00000003.322437371.0000000005E1F 000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	file.exe, 00000000.00000003.328186440.00 00000005DED000.00000004.00000800.0002000 0.00000000.sdmp	false		high
http://www.goodfont.co.kr	file.exe, 00000000.00000002.372638789.00 00000006FE2000.00000004.00000800.0002000 0.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	file.exe, 00000000.00000003.323364666.00 00000005DFD000.00000004.00000800.0002000 0.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn9)z	file.exe, 00000000.00000003.322190648.00 00000005DFB000.00000004.00000800.0002000 0.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersR	file.exe, 00000000.00000003.328259813.00 00000005DED000.00000004.00000800.0002000 0.00000000.sdmp	false		high
http://www.sajatypeworks.com	file.exe, 00000000.00000002.372638789.00 00000006FE2000.00000004.00000800.0002000 0.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.org4	file.exe, 00000003.00000002.588190939.00 00000003216000.00000004.00000800.0002000 0.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	file.exe, 00000000.00000002.372638789.00 00000006FE2000.00000004.00000800.0002000 0.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	file.exe, 00000000.00000002.372638789.00 00000006FE2000.00000004.00000800.0002000 0.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	file.exe, 00000000.00000003.331573813.00 00000005DDE000.00000004.00000800.0002000 0.00000000.sdmp, file.exe, 00000000.0000 0003.332017649.0000000005DDE000.00000004 .00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.331737193.00000000 05DDE000.00000004.00000800.00020000.0000 0000.sdmp, file.exe, 00000000.00000002.3 72638789.0000000006FE2000.00000004.00000 800.00020000.00000000.sdmp, file.exe, 00 000000.00000003.331448993.0000000005DDE0 00.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.331935801.0000000 005DDE000.00000004.00000800.00020000.000 00000.sdmp, file.exe, 00000000.00000003. 331515934.0000000005DDE000.00000004.0000 0800.00020000.00000000.sdmp, file.exe, 0 0000000.00000003.332325766.0000000005DDE 000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.331681925.0000000 0005DDE000.00000004.00000800.00020000.00 000000.sdmp, file.exe, 00000000.00000003 .331804071.0000000005DDE000.00000004.000 00800.00020000.00000000.sdmp, file.exe, 00000000.00000003.332125875.0000000005DD E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.332245431.00000 00005DDE000.00000004.00000800.00020000.0 0000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	file.exe, 00000000.00000002.372638789.00 00000006FE2000.00000004.00000800.0002000 0.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/q	file.exe, 00000000.00000002.367556703.00000000004135000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.370182647.000000000445D000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000003.00000000.356501796.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de2	file.exe, 00000000.00000003.325755043.00000005DDE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.325630110.0000000005DDE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.325677616.0000000005DDE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn_	file.exe, 00000000.00000003.322004645.00000005DDC000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.322247274.0000000005DDD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	file.exe, 00000000.00000002.372638789.00000006FE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	file.exe, 00000000.00000002.372638789.00000006FE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	file.exe, 00000000.00000002.372638789.00000006FE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.com	file.exe, 00000003.00000002.588227793.00000003222000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	file.exe, 00000000.00000002.372638789.00000006FE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	file.exe, 00000000.00000003.325630110.00000005DDE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.325677616.0000000005DDE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.dewa	file.exe, 00000000.00000003.325630110.00000005DDE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.325677616.0000000005DDE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	file.exe, 00000000.00000003.323222872.00000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323273225.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323456584.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.322784264.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.372638789.0000000006FE2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.322849771.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.322819666.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323165080.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323364666.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com#	file.exe, 00000000.00000003.322314879.00000005E1E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	file.exe, 00000003.00000002.587378130.00000003181000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.como.	file.exe, 00000000.00000003.323222872.00000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323273225.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323456584.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.322849771.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323165080.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323364666.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	file.exe, 00000000.00000002.372638789.00000006FE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	file.exe, 00000000.00000002.372638789.00000006FE2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.322654693.0000000005DE6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	file.exe, 00000000.00000002.372638789.00000006FE2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.357757128.0000000005DD0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	file.exe, 00000000.00000003.331690866.00000005DE7000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.331745202.0000000005DE8000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.331466240.0000000005DE5000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.331580926.0000000005DE7000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.331524670.0000000005DE5000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.331820779.0000000005DE7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.htmlh	file.exe, 00000000.00000003.327061644.00000005DEC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.come	file.exe, 00000000.00000003.323222872.00000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323273225.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323456584.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323165080.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323364666.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comTC	file.exe, 00000000.00000003.323364666.00000005DFD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comn	file.exe, 00000000.00000003.322410540.00000005E1E000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.322390325.0000000005E1E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.org	file.exe, 00000003.00000002.588190939.00000003216000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000003.00000002.588227793.0000000003222000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comt	file.exe, 00000000.00000003.323222872.00000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323273225.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323456584.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323165080.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323364666.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cne	file.exe, 00000000.00000003.322784264.00000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.322849771.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.322819666.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	file.exe, 00000000.00000003.321085020.00000005DFC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	file.exe, 00000000.00000002.372638789.00000006FE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	file.exe, 00000000.00000003.322190648.00000005DFB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	file.exe, 00000000.00000002.372638789.00000006FE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comuctP	file.exe, 00000000.00000003.323273225.00000005DFD000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.323364666.0000000005DFD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers&	file.exe, 00000000.00000003.326503329.00000005DEA000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.327161655.0000000005DEC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	file.exe, 00000000.00000003.322004645.00000005DDC000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000002.372638789.0000000006FE2000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.322040067.0000000005DFA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.dew	file.exe, 00000000.00000003.325630110.00000005DDE000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.325677616.0000000005DDE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	file.exe, 00000000.00000002.372638789.00000006FE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comoitu	file.exe, 00000000.00000003.357757128.00000005DD0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	file.exe, 00000000.00000003.327948700.00000005DED000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnn-uAofz	file.exe, 00000000.00000003.322004645.00000005DDC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.	file.exe, 00000000.00000003.338369032.00000005DF7000.00000004.00000800.00020000.00000000.sdmp, file.exe, 00000000.00000003.338650954.0000000005DF7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	file.exe, 00000000.00000002.372638789.00000006FE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	file.exe, 00000000.00000002.372638789.00000006FE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/h	file.exe, 00000000.00000003.325835624.00000005DE3000.00000004.00000800.00020000.00000000.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	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756297
Start date and time:	2022-11-30 00:10:13 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	9
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@8/1@2/2

Copyright Joe Security LLC 2022

EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
00:11:25	API Interceptor	1x Sleep call for process: file.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\file.exe.log

Process:	C:\Users\user\Desktop\file.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):	7.5108050447651635
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	file.exe
File size:	749056
MD5:	cfc1c66cba07daef1e8ac13d5e042e7a
SHA1:	10451947894a7af9a06adc619179e00e933fb20a
SHA256:	addc1564d69b115e0cb5ff2264614c98dc51107f042e3ea0d93b99e49cf2e94b
SHA512:	40972496a2f5d3f2b2b408c90ef026a7c7df040f31af793da63406c37688278a40f011d28dca9c976c1d566fe28768643d374dae4f9e1967919ee87018492bd5
SSDEEP:	12288:WOvVmqjryPp7LCMYFx6sdzSEACiy4lCfUZ/4J8wRdd0/Ok9:5mqj0xEkyWCfUt4J8wDdo
TLSH:	41F4292297B1C906F93389ED62EC5A014DA860C158B4C949CC573DC05E78E6BF5FCAFA
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..f..... .....@.. .....@.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b84fa
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:	0xA1D69E9C [Sat Jan 15 21:24:44 2056 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

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

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb6500	0xb6600	False	0.7620373543522961	data	7.516664543280966	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xba000	0x370	0x400	False	0.36328125	data	2.7767798139639406	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbc000	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	0xba058	0x314	data		

Imports

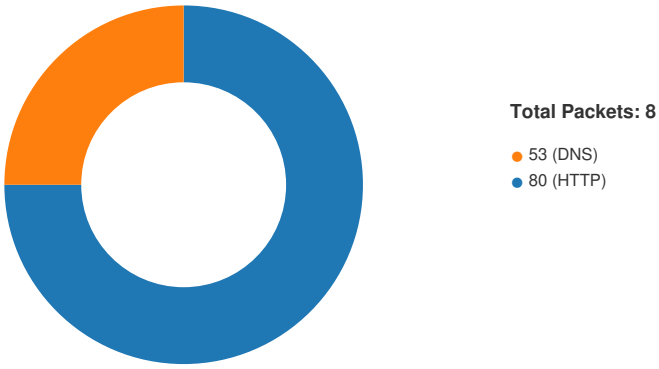
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4193.122.130.0 49696802039190 11/30/22-00:11:36.516564	TCP	2039190	ET TROJAN 404/Snake/Matiex Keylogger Style External IP Check	49696	80	192.168.2.4	193.122.130.0

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:11:36.409488916 CET	49696	80	192.168.2.4	193.122.130.0
Nov 30, 2022 00:11:36.515891075 CET	80	49696	193.122.130.0	192.168.2.4
Nov 30, 2022 00:11:36.516032934 CET	49696	80	192.168.2.4	193.122.130.0
Nov 30, 2022 00:11:36.516563892 CET	49696	80	192.168.2.4	193.122.130.0
Nov 30, 2022 00:11:36.623718977 CET	80	49696	193.122.130.0	192.168.2.4
Nov 30, 2022 00:11:36.624381065 CET	80	49696	193.122.130.0	192.168.2.4
Nov 30, 2022 00:11:36.726608992 CET	49696	80	192.168.2.4	193.122.130.0
Nov 30, 2022 00:12:41.628427029 CET	80	49696	193.122.130.0	192.168.2.4

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:12:41.631309032 CET	49696	80	192.168.2.4	193.122.130.0
Nov 30, 2022 00:13:16.671070099 CET	49696	80	192.168.2.4	193.122.130.0
Nov 30, 2022 00:13:16.779337883 CET	80	49696	193.122.130.0	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:11:36.306314945 CET	56572	53	192.168.2.4	8.8.8.8
Nov 30, 2022 00:11:36.323108912 CET	53	56572	8.8.8.8	192.168.2.4
Nov 30, 2022 00:11:36.351854086 CET	50911	53	192.168.2.4	8.8.8.8
Nov 30, 2022 00:11:36.369916916 CET	53	50911	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 00:11:36.306314945 CET	192.168.2.4	8.8.8.8	0xd6ad	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:36.351854086 CET	192.168.2.4	8.8.8.8	0xb47e	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)	false

DNS Answers

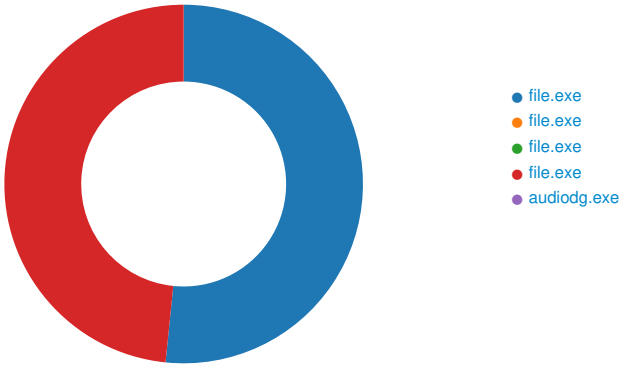
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:11:36.323108912 CET	8.8.8.8	192.168.2.4	0xd6ad	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 00:11:36.323108912 CET	8.8.8.8	192.168.2.4	0xd6ad	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:36.323108912 CET	8.8.8.8	192.168.2.4	0xd6ad	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:36.323108912 CET	8.8.8.8	192.168.2.4	0xd6ad	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:36.323108912 CET	8.8.8.8	192.168.2.4	0xd6ad	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:36.323108912 CET	8.8.8.8	192.168.2.4	0xd6ad	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:36.369916916 CET	8.8.8.8	192.168.2.4	0xb47e	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 00:11:36.369916916 CET	8.8.8.8	192.168.2.4	0xb47e	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:36.369916916 CET	8.8.8.8	192.168.2.4	0xb47e	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:36.369916916 CET	8.8.8.8	192.168.2.4	0xb47e	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:36.369916916 CET	8.8.8.8	192.168.2.4	0xb47e	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:11:36.369916916 CET	8.8.8.8	192.168.2.4	0xb47e	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- checkip.dyndns.org

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: file.exe PID: 1128, Parent PID: 3528

General

Target ID:	0
Start time:	00:11:13
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0xaa0000
File size:	749056 bytes
MD5 hash:	CFC1C66CBA07DAEF1E8AC13D5E042E7A
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: 00000000.00000002.365680487.0000000003439000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.367556703.0000000004135000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000002.367556703.0000000004135000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.367556703.0000000004135000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000002.367556703.0000000004135000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_SnakeKeylogger_af3faa65, Description: unknown, Source: 00000000.00000002.367556703.0000000004135000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.370182647.000000000445D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000002.370182647.000000000445D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.370182647.000000000445D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000002.370182647.000000000445D000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_SnakeKeylogger_af3faa65, Description: unknown, Source: 00000000.00000002.370182647.000000000445D000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	6D63CF06	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	6D63CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\file.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D94C78D	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\file.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	6D94C907	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	6D615705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D615705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D61CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D615705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D615705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C481B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C481B4F	ReadFile

Analysis Process: file.exe PID: **5916**, Parent PID: **1128**

General	
Target ID:	1
Start time:	00:11:29
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x390000
File size:	749056 bytes
MD5 hash:	CFC1C66CBA07DAEF1E8AC13D5E042E7A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: file.exe PID: **4844**, Parent PID: **1128**

General	
Target ID:	2
Start time:	00:11:31
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x350000
File size:	749056 bytes
MD5 hash:	CFC1C66CBA07DAEF1E8AC13D5E042E7A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: file.exe PID: **5260**, Parent PID: **1128**

General	
Target ID:	3
Start time:	00:11:32
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0xd80000
File size:	749056 bytes
MD5 hash:	CFC1C66CBA07DAEF1E8AC13D5E042E7A
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: 00000003.00000000.356501796.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000003.00000000.356501796.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.356501796.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000003.00000000.356501796.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_SnakeKeylogger_af3faa65, Description: unknown, Source: 00000003.00000000.356501796.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
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	6D63CF06	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	6D63CF06	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	6D615705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D615705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D61CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D615705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D615705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C481B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C481B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C481B4F	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

Analysis Process: audiodg.exe PID: **4844**, Parent PID: **1596**

General

Target ID:	8
Start time:	00:13:01
Start date:	30/11/2022
Path:	C:\Windows\System32\audiodg.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\AUDIODG.EXE 0x364
Imagebase:	0x7ff6fc6d0000
File size:	594128 bytes
MD5 hash:	0B245353F92DF527AA7613BA2C0DA023
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Copyright Joe Security LLC 2022

Disassembly

No disassembly