ID: 708246
Sample Name: P0A2249.exe
Cookbook: default.jbs
Time: 08:10:13
Date: 23/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

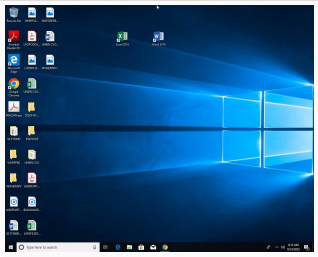
Windows Analysis Report

P0A2249.exe

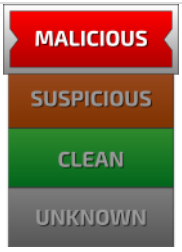
Overview

General Information

Sample Name:	P0A2249.exe
Analysis ID:	708246
MD5:	43f9694be950da..
SHA1:	2138532f5a0938..
SHA256:	aa42f20183026e..
Tags:	exe SnakeKeylogger
Infos:	



Detection



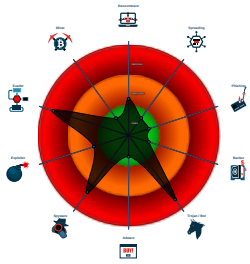
Snake Keylogger

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
- 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…
- May check the online IP address of…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- P0A2249.exe (PID: 5572 cmdline: "C:\Users\user\Desktop\P0A2249.exe" MD5: 43F9694BE950DA3CBC89CEB296B2EB3B)
  - P0A2249.exe (PID: 6092 cmdline: C:\Users\user\Desktop\P0A2249.exe MD5: 43F9694BE950DA3CBC89CEB296B2EB3B)
- **cleanup**

Malware Configuration

Threatname: Snake Keylogger


```
{
  "Exfil Mode": "Telegram",
  "Telegram Token": "5478319803:AAHq9LkDUFBRvjOub4YfRlPURZxM59_BVnc",
  "Telegram ID": "5516439768"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.267679195.000000000384B000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
00000000.00000002.267679195.000000000384B000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
00000000.00000002.267679195.000000000384B000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.267679195.000000000384B000.00000004.00000800.00020000.00000000.sdmp	MALWARE_Win_SnakeKeylogger	Detects Snake Keylogger	ditekSHen	• 0x50e04:$x1: $%SMTPDV$ • 0x70424:$x1: $%SMTPDV$ • 0x4fac6:$x2: $#TheHashHere%& • 0x6f0e6:$x2: $#TheHashHere%& • 0x50dac:$x3: %FTPDV$ • 0x703cc:$x3: %FTPDV$ • 0x4faa8:$x4: $%TelegramDv$ • 0x6f0c8:$x4: $%TelegramDv$ • 0x4d437:$x5: KeyLoggerEventArgs • 0x4d7cd:$x5: KeyLoggerEventArgs • 0x6ca57:$x5: KeyLoggerEventArgs • 0x6cded:$x5: KeyLoggerEventArgs • 0x50e30:$m1: \| Snake Keylogger • 0x50ed6:$m1: | Snake Keylogger • 0x5102a:$m1: \| Snake Keylogger • 0x51150:$m1: | Snake Keylogger • 0x512aa:$m1: \| Snake Keylogger • 0x70450:$m1: | Snake Keylogger • 0x704f6:$m1: \| Snake Keylogger • 0x7064a:$m1: | Snake Keylogger • 0x70770:$m1: | Snake Keylogger
00000000.00000002.267679195.000000000384B000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_SnakeKeylogger_af3faa65	unknown	unknown	• 0x4c241:$a1: get_encryptedPassword • 0x6b861:$a1: get_encryptedPassword • 0x4c52d:$a2: get_encryptedUsername • 0x6bb4d:$a2: get_encryptedUsername • 0x4c04d:$a3: get_timePasswordChanged • 0x6b66d:$a3: get_timePasswordChanged • 0x4c148:$a4: get_passwordField • 0x6b768:$a4: get_passwordField • 0x4c257:$a5: set_encryptedPassword • 0x6b877:$a5: set_encryptedPassword • 0x4d86a:$a7: get_logins • 0x6ce8a:$a7: get_logins • 0x4d7cd:$a10: KeyLoggerEventArgs • 0x6cded:$a10: KeyLoggerEventArgs • 0x4d437:$a11: KeyLoggerEventArgsEventHandler • 0x6ca57:$a11: KeyLoggerEventArgsEventHandler
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.P0A2249.exe.3883640.10.raw.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x1b0c4:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x3a6e4:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x1a2ad:$a3: \Google\Chrome\User Data\Default\Login Data • 0x398cd:$a3: \Google\Chrome\User Data\Default\Login Data • 0x1a6f4:$a4: \Orbitum\User Data\Default\Login Data • 0x39d14:$a4: \Orbitum\User Data\Default\Login Data • 0x1b875:$a5: \Kometa\User Data\Default\Login Data • 0x3ae95:$a5: \Kometa\User Data\Default\Login Data
0.2.P0A2249.exe.3883640.10.raw.unpack	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
0.2.P0A2249.exe.3883640.10.raw.unpack	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
0.2.P0A2249.exe.3883640.10.raw.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
0.2.P0A2249.exe.3883640.10.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 38 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN 404/Snake/Matiex Keylogger Style External IP Check - Source IP: 192.168.2.3 - Destination IP: 193.122.130.0	
Timestamp:	192.168.2.3193.122.130.049702802842536 09/23/22-08:11:16.993448
SID:	2842536
Source Port:	49702
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

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

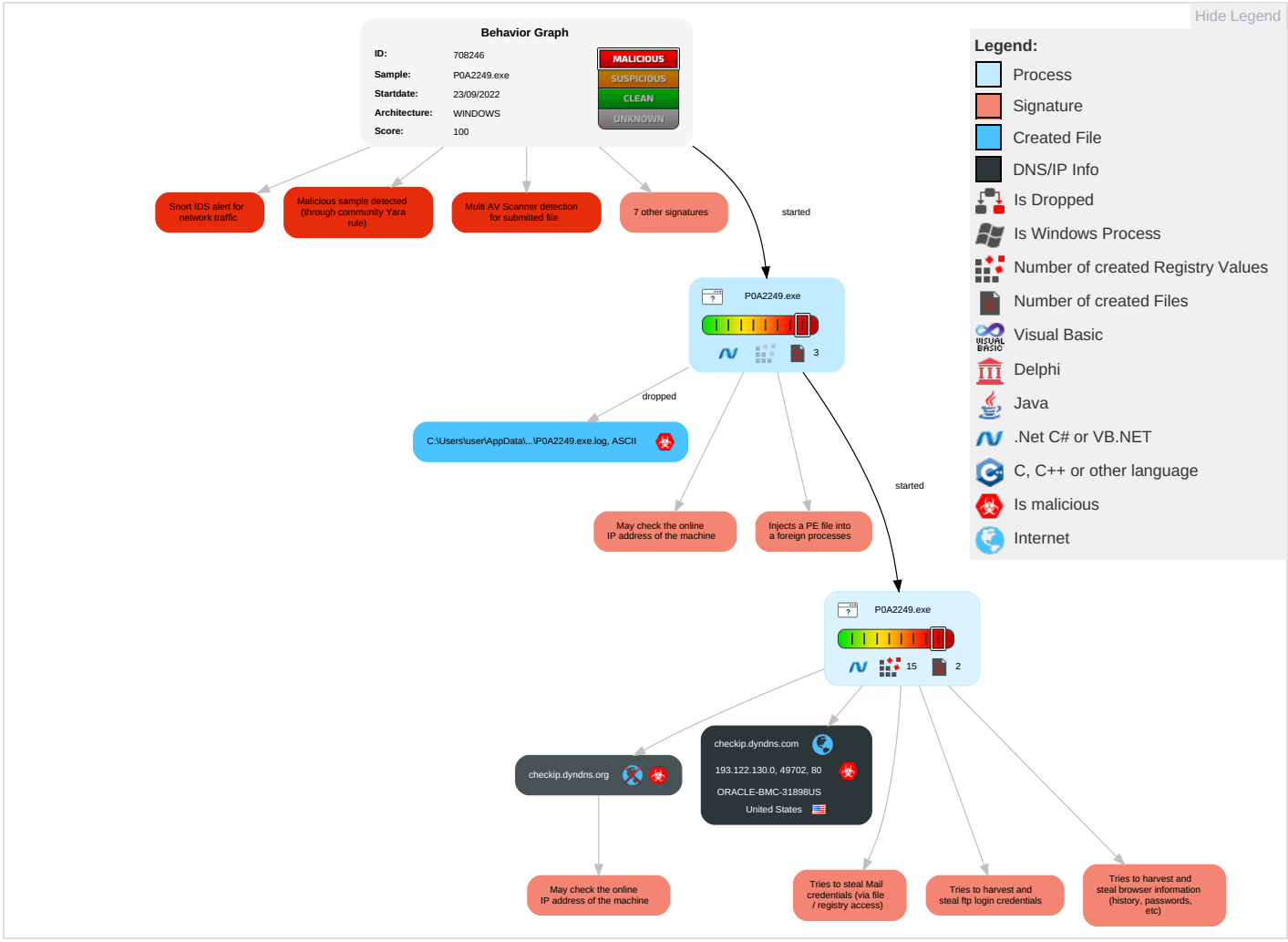
Yara detected Snake Keylogger

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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Application Window 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 Remote System 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 System Network Configuration 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	1 3 System Information Discovery	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
P0A2249.exe	18%	ReversingLabs	ByteCode-MSIL.Packed.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.P0A2249.exe.400000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
0.2.P0A2249.exe.34b5928.9.unpack	100%	Avira	HEUR/AGEN.1244307		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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://checkip.dyndns.org	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://checkip.dyndns.org4Rk0%	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://checkip.dyndns.org/	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTF	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://checkip.dyndns.org/q	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	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.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnP&br	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnT%~s	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnZ&xr	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnb%0s	0%	Avira URL Cloud	safe	
http://www.tiro.comO	0%	Avira URL Cloud	safe	
http://www.sakkal.comu	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	true	• 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/	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

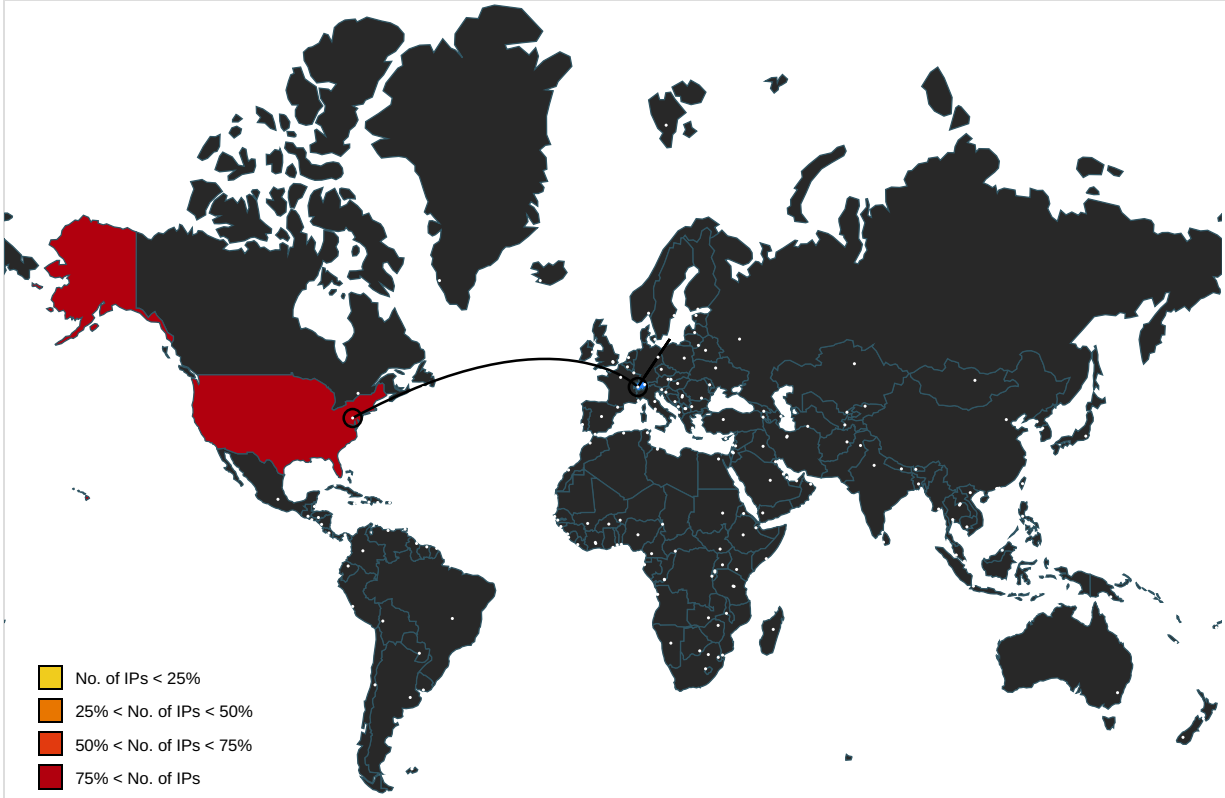
Name	Source	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org4Rk0%	P0A2249.exe, 00000001.00000002.509786023.0000000030C4000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	P0A2249.exe, 00000000.00000002.274934321.000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	P0A2249.exe, 00000000.00000002.274934321.000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot	P0A2249.exe, 00000000.00000002.267679195.000000000384B000.00000004.00000800.00020000.00000000.sdmp, P0A2249.exe, 00000000.00000002.265747551.00000000034B5000.00000004.00000800.00020000.00000000.sdmp, P0A2249.exe, 00000001.00000000.260243480.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/frere-jones.html.	P0A2249.exe, 00000000.00000003.248064801.0000000005927000.00000004.00000800.00020000.00000000.sdmp, P0A2249.exe, 00000000.00000003.248032820.0000000005926000.00000004.00000800.00020000.00000000.sdmp, P0A2249.exe, 00000000.00000003.248091025.0000000005927000.00000004.00000800.00020000.00000000.sdmp, P0A2249.exe, 00000000.00000003.248048236.0000000005926000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.org	P0A2249.exe, 00000001.00000002.509834203.00000000030D1000.00000004.00000800.00020000.00000000.sdmp, P0A2249.exe, 00000001.00000002.509786023.00000000030C4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnP&br	P0A2249.exe, 00000000.00000003.245640025.00000000058F2000.00000004.00000800.00020000.00000000.sdmp, P0A2249.exe, 00000000.00000003.245514997.00000000058FB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	P0A2249.exe, 00000000.00000003.262445246.00000000058F0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.comu	P0A2249.exe, 00000000.00000003.247064033.0000000005926000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	P0A2249.exe, 00000000.00000003.245640025.00000000058F2000.00000004.00000800.00020000.00000000.sdmp, P0A2249.exe, 00000000.00000003.245133873.00000000058FC000.00000004.00000800.00020000.00000000.sdmp, P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp, P0A2249.exe, 00000000.00000003.245514997.00000000058FB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comB.TTF	P0A2249.exe, 00000000.00000003.262445246.00000000058F0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.monotype.	P0A2249.exe, 00000000.00000003.251458280.0000000005929000.00000004.00000800.00020000.00000000.sdmp, P0A2249.exe, 00000000.00000003.251535004.000000000592D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comO	P0A2249.exe, 00000000.00000003.245640025.00000000058F2000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://checkip.dyndns.org/q	P0A2249.exe, 00000000.00000002.267679195.000000000384B000.00000004.00000800.00020000.00000000.sdmp, P0A2249.exe, 00000000.00000002.265747551.00000000034B5000.00000004.00000800.00020000.00000000.sdmp, P0A2249.exe, 00000001.00000000.260243480.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	P0A2249.exe, 00000000.00000003.242838731.00000000058F3000.00000004.00000800.00020000.00000000.sdmp, P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.com	P0A2249.exe, 00000001.00000002.509834203.00000000030D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnT%~s	P0A2249.exe, 00000000.00000003.245640025.00000000058F2000.00000004.00000800.00020000.00000000.sdmp, P0A2249.exe, 00000000.00000003.245514997.00000000058FB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnZ&xr	P0A2249.exe, 00000000.00000003.245640025.00000000058F2000.00000004.00000800.00020000.00000000.sdmp, P0A2249.exe, 00000000.00000003.245514997.00000000058FB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	P0A2249.exe, 00000000.00000002.263992516.0000000002471000.00000004.00000800.00020000.00000000.sdmp, P0A2249.exe, 00000001.00000002.509215659.0000000003031000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	P0A2249.exe, 00000000.00000003.247049588.0000000005926000.00000004.00000800.00020000.00000000.sdmp, P0A2249.exe, 00000000.00000002.274934321.0000000006B82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnb%0s	P0A2249.exe, 00000000.00000003.245133873.00000000058FC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

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

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	708246
Start date and time:	2022-09-23 08:10:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	P0A2249.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:	13
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@3/1
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, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com
- 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
08:11:04	API Interceptor	84x Sleep call for process: P0A2249.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\P0A2249.exe.log

Process:	C:\Users\user\Desktop\P0A2249.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1394
Entropy (8bit):	5.340883346054895
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4KnKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84F0:MIHK5HKXE1qHbHKnYHKhQnoPtHoxHhAR

MD5:	B51A52A837298BCF7A6EB58551AEF99C
SHA1:	61EEFCC20AC255B8651769E5C48E27B2A983FC4A
SHA-256:	1D393FBB3CE754EA699462C2778587A7F2451EB23BE2BD5084C95A46B20BE8AF
SHA-512:	138544399787651C847837719606197E539857206CCB271E0F4A86E2017FBADABADF5A235B6F6F1DA8ADE7EF29DBA3115CD1996AD01F92CA30C57D0BF217C11
Malicious:	**true**
Reputation:	moderate, 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..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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=b77a5c561934e08

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.616410424839483
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:	P0A2249.exe
File size:	1191424
MD5:	43f9694be950da3cbc89ceb296b2eb3b
SHA1:	2138532f5a09386b06a338acab2b79b0167b7f62
SHA256:	aa42f20183026e8912e487dc655d4459e8e37e3743cdc7753dc60fa712d8117f
SHA512:	f6dedfc5b460f7eddbee51f4d0b98490a4b7f0791a573f803823d5444c52519bed0dcbaa73b213ff826b3a5a00c0822adde87301268fa350567285f22d0240ac
SSDEEP:	12288:0hLuyAHYT68OXKtHRtD4/coF8IxbVp2w2L6TVHLT0R2pmMCTi:0hLuyyW65X2k/F8nw2cHLTU6C
TLSH:	FD457E92B1908D9BE86B16F1AC66D53012E7AD5C94A4C10D5ADABF1F71F3342209FF0E
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...+.....0.....J.... .....@.. .....@.....

File Icon

Icon Hash:	aeacae8eb6a2be00

Static PE Info

General

Entrypoint:	0x4dbf4a
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:	0xA2A7912B [Thu Jun 22 09:11:07 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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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 al, 00h
add byte ptr [eax], al
add byte ptr [eax], al
add eax, dword ptr [eax]
add eax, dword ptr [eax]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xdbef8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xdc000	0x488c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x126000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xdbedc	0x1c	.text
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	0xd9f50	0xda000	False	0.7176838446100917	data	6.919011980791601	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xdc000	0x488c8	0x48a00	False	0.062308385327022375	data	4.758656767526677	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x126000	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_ICON	0xdc298	0x668	data		
RT_ICON	0xdc900	0x2e8	data		
RT_ICON	0xdcbe8	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0xdcd10	0xea8	data		
RT_ICON	0xddbb8	0x8a8	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xde460	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0xde9c8	0x42028	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x1209f0	0x25a8	data		
RT_ICON	0x122f98	0x10a8	data		
RT_ICON	0x124040	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1244a8	0x92	data		
RT_VERSION	0x12453c	0x38c	PGP symmetric key encrypted data - Plaintext or unencrypted data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3193.122.130.0 49702802842536 09/23/22-08:11:16.993448	TCP	2842536	ETPRO TROJAN 404/Snake/Matiex Keylogger Style External IP Check	49702	80	192.168.2.3	193.122.130.0

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 08:11:16.876717091 CEST	49702	80	192.168.2.3	193.122.130.0
Sep 23, 2022 08:11:16.984992981 CEST	80	49702	193.122.130.0	192.168.2.3
Sep 23, 2022 08:11:16.987874985 CEST	49702	80	192.168.2.3	193.122.130.0
Sep 23, 2022 08:11:16.993448019 CEST	49702	80	192.168.2.3	193.122.130.0
Sep 23, 2022 08:11:17.101823092 CEST	80	49702	193.122.130.0	192.168.2.3
Sep 23, 2022 08:11:17.103646040 CEST	80	49702	193.122.130.0	192.168.2.3
Sep 23, 2022 08:11:17.152368069 CEST	49702	80	192.168.2.3	193.122.130.0
Sep 23, 2022 08:12:22.103549957 CEST	80	49702	193.122.130.0	192.168.2.3
Sep 23, 2022 08:12:22.103838921 CEST	49702	80	192.168.2.3	193.122.130.0
Sep 23, 2022 08:12:57.146246910 CEST	49702	80	192.168.2.3	193.122.130.0
Sep 23, 2022 08:12:57.254538059 CEST	80	49702	193.122.130.0	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 23, 2022 08:11:15.790663004 CEST	49977	53	192.168.2.3	8.8.8.8
Sep 23, 2022 08:11:15.808007002 CEST	53	49977	8.8.8.8	192.168.2.3
Sep 23, 2022 08:11:15.828238010 CEST	57840	53	192.168.2.3	8.8.8.8
Sep 23, 2022 08:11:16.841366053 CEST	57840	53	192.168.2.3	8.8.8.8
Sep 23, 2022 08:11:16.860634089 CEST	53	57840	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 23, 2022 08:11:15.790663004 CEST	192.168.2.3	8.8.8.8	0xf46e	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)	false
Sep 23, 2022 08:11:15.828238010 CEST	192.168.2.3	8.8.8.8	0x98b9	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)	false
Sep 23, 2022 08:11:16.841366053 CEST	192.168.2.3	8.8.8.8	0x98b9	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
Sep 23, 2022 08:11:15.808007002 CEST	8.8.8.8	192.168.2.3	0xf46e	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)	false
Sep 23, 2022 08:11:15.808007002 CEST	8.8.8.8	192.168.2.3	0xf46e	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)	false
Sep 23, 2022 08:11:15.808007002 CEST	8.8.8.8	192.168.2.3	0xf46e	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Sep 23, 2022 08:11:15.808007002 CEST	8.8.8.8	192.168.2.3	0xf46e	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)	false
Sep 23, 2022 08:11:15.808007002 CEST	8.8.8.8	192.168.2.3	0xf46e	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)	false
Sep 23, 2022 08:11:15.808007002 CEST	8.8.8.8	192.168.2.3	0xf46e	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)	false
Sep 23, 2022 08:11:16.860634089 CEST	8.8.8.8	192.168.2.3	0x98b9	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)	false
Sep 23, 2022 08:11:16.860634089 CEST	8.8.8.8	192.168.2.3	0x98b9	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)	false
Sep 23, 2022 08:11:16.860634089 CEST	8.8.8.8	192.168.2.3	0x98b9	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)	false
Sep 23, 2022 08:11:16.860634089 CEST	8.8.8.8	192.168.2.3	0x98b9	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)	false
Sep 23, 2022 08:11:16.860634089 CEST	8.8.8.8	192.168.2.3	0x98b9	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)	false
Sep 23, 2022 08:11:16.860634089 CEST	8.8.8.8	192.168.2.3	0x98b9	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- checkip.dyndns.org

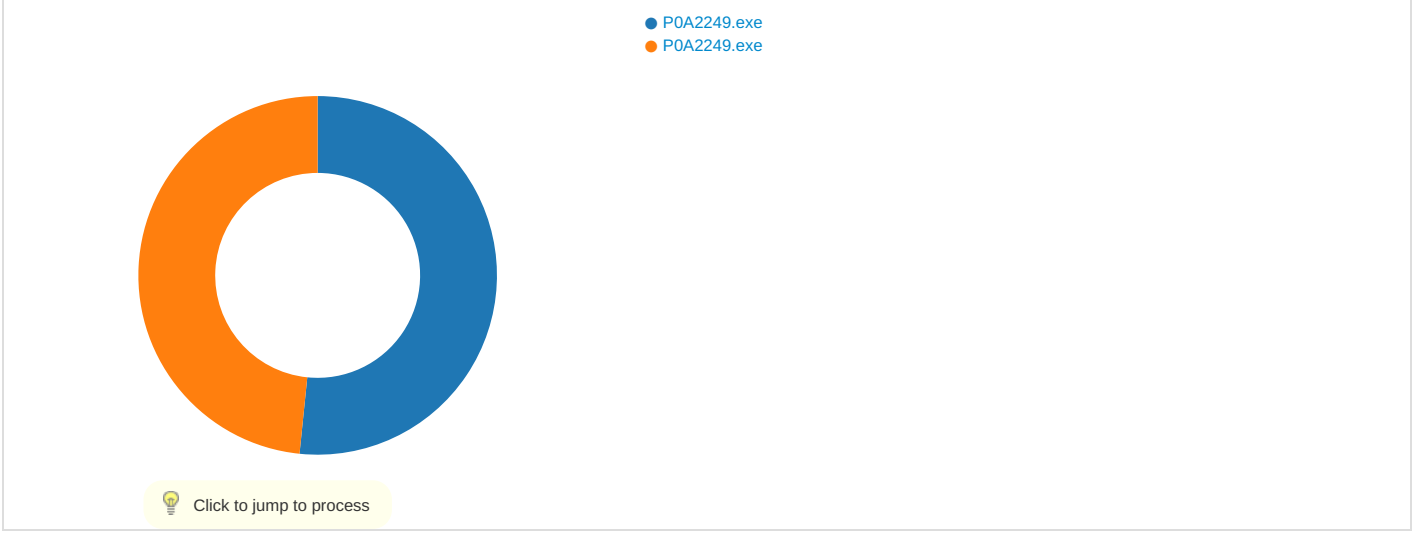
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49702	193.122.130.0	80	C:\Users\user\Desktop\P0A2249.exe

Timestamp	kBytes transferred	Direction	Data
Sep 23, 2022 08:11:16.993448019 CEST	102	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
Sep 23, 2022 08:11:17.103646040 CEST	102	IN	HTTP/1.1 200 OK Date: Fri, 23 Sep 2022 06:11:17 GMT Content-Type: text/html Content-Length: 103 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 38 34 2e 31 37 2e 35 32 2e 34 33 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: 84.17.52.43</body></html>

Statistics

Behavior



System Behavior

Analysis Process: P0A2249.exe PID: **5572**, Parent PID: **5308**

General

Target ID:	0
Start time:	08:11:03
Start date:	23/09/2022
Path:	C:\Users\user\Desktop\P0A2249.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\P0A2249.exe"
Imagebase:	0x70000
File size:	1191424 bytes
MD5 hash:	43F9694BE950DA3CBC89CEB296B2EB3B
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: 00000000.00000002.267679195.000000000384B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000002.267679195.000000000384B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.267679195.000000000384B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000002.267679195.000000000384B000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_SnakeKeylogger_af3faa65, Description: unknown, Source: 00000000.00000002.267679195.000000000384B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.264198138.00000000024C8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.265747551.00000000034B5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000002.265747551.00000000034B5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.265747551.00000000034B5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000002.265747551.00000000034B5000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_SnakeKeylogger_af3faa65, Description: unknown, Source: 00000000.00000002.265747551.00000000034B5000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D38CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D38CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\P0A2249.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\P0A2249.exe.log	0	1394	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	6D69C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile

Analysis Process: P0A2249.exe PID: **6092**, Parent PID: **5572**

General

Target ID:	1
Start time:	08:11:12
Start date:	23/09/2022
Path:	C:\Users\user\Desktop\P0A2249.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\P0A2249.exe
Imagebase:	0xbb0000
File size:	1191424 bytes
MD5 hash:	43F9694BE950DA3CBC89CEB296B2EB3B
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: 00000001.00000000.260243480.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000001.00000000.260243480.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.260243480.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000001.00000000.260243480.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_SnakeKeylogger_af3faa65, Description: unknown, Source: 00000001.00000000.260243480.0000000000402000.00000040.00000400.00020000.00000000.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	6D38CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D38CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C1D1B4F	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