



ID: 356841
Sample Name:
PO202100046.exe
Cookbook: default.jbs
Time: 17:40:32
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report PO202100046.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Snake Keylogger 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Compliance: 5
Networking: 5
Data Obfuscation: 6
Malware Analysis System Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 10
Public 10
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 13
ASN 14
JA3 Fingerprints 14
Dropped Files 15
Created / dropped Files 15
Static File Info 15
General 15
File Icon 16
Static PE Info 16
General 16
Entrypoint Preview 16
Data Directories 18
Sections 18

Copyright null 2021

Resources 18
Imports 18
Version Infos 18
Network Behavior 19
Network Port Distribution 19
TCP Packets 19
UDP Packets 20
DNS Queries 21
DNS Answers 21
HTTP Request Dependency Graph 22
HTTP Packets 22
HTTPS Packets 22
Code Manipulations 23
Statistics 23
Behavior 23
System Behavior 23
Analysis Process: PO202100046.exe PID: 6952 Parent PID: 5848 23
General 23
File Activities 24
File Created 24
File Written 24
File Read 24
Analysis Process: PO202100046.exe PID: 6988 Parent PID: 6952 25
General 25
File Activities 25
File Created 25
File Deleted 25
File Read 25
Registry Activities 26
Disassembly 26
Code Analysis 26

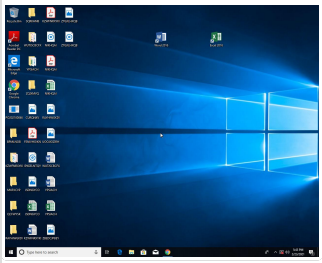
Analysis Report PO202100046.exe

Overview

General Information

Sample Name:	PO202100046.exe
Analysis ID:	356841
MD5:	eafc433b4d4bf4a..
SHA1:	0ba21c1f4f908e5..
SHA256:	77ee17838c1ea6..
Tags:	exe SnakeKeylogger
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

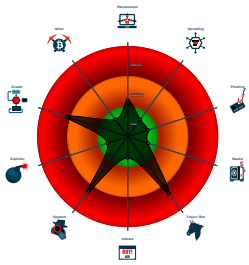
Snake Keylogger

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Snake Keylogger
- Binary contains a suspicious time st…
- Machine Learning detection for samp…
- May check the online IP address of …
- Tries to harvest and steal browser in…
- Tries to steal Mail credentials (via fil…
- Yara detected Beds Obfuscator
- Antivirus or Machine Learning detec…
- Contains functionality to access load…
- Contains long sleeps (>= 3 min)
- Creates a DirectInput object (often fo…
- Creates a process in suspended mo…

Classification



Startup

- **System is w10x64**
- PO202100046.exe (PID: 6952 cmdline: 'C:\Users\user\Desktop\PO202100046.exe' MD5: EAFC433B4D4BF4A0EDC9B57B6F4AF8EC)
  - PO202100046.exe (PID: 6988 cmdline: C:\Users\user\Desktop\PO202100046.exe MD5: EAFC433B4D4BF4A0EDC9B57B6F4AF8EC)
- **cleanup**

Malware Configuration

Threatname: Snake Keylogger

```
{
  "Exfil Mode": "Telegram",
  "Telegram Info": {
    "Telegram ID": "1556351268",
    "Telegram Token": "1591373451:AAH6Q2mvjdA9146Wl0khv2-kuh-iTps2zjw"
  }
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.325194217.0000000004A90000.00000004.00000001.sdmp	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
00000000.00000003.319958198.0000000004C71000.00000004.00000001.sdmp	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
00000000.00000003.319958198.0000000004C71000.00000004.00000001.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
00000000.00000002.323967870.0000000003489000.00000004.00000001.sdmp	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.323967870.000000000348 9000.00000004.00000001.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
Click to see the 7 entries				

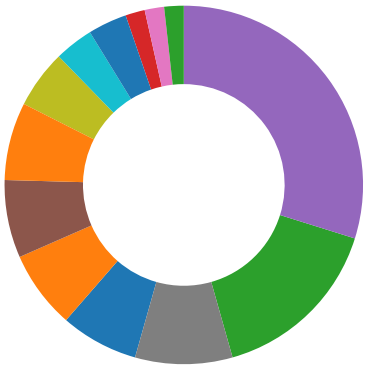
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PO202100046.exe.35ae570.3.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
0.2.PO202100046.exe.4a90000.8.raw.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
0.2.PO202100046.exe.351bd40.5.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
0.2.PO202100046.exe.4a90000.8.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
0.2.PO202100046.exe.36a37b8.4.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
Click to see the 9 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:



Uses 32bit PE files

Uses insecure TLS / SSL version for HTTPS connection

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:



Copyright null 2021

May check the online IP address of the machine

Data Obfuscation:



Binary contains a suspicious time stamp

Yara detected Beds Obfuscator

Malware Analysis System Evasion:



Yara detected Beds Obfuscator

Stealing of Sensitive Information:



Yara detected Snake Keylogger

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

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

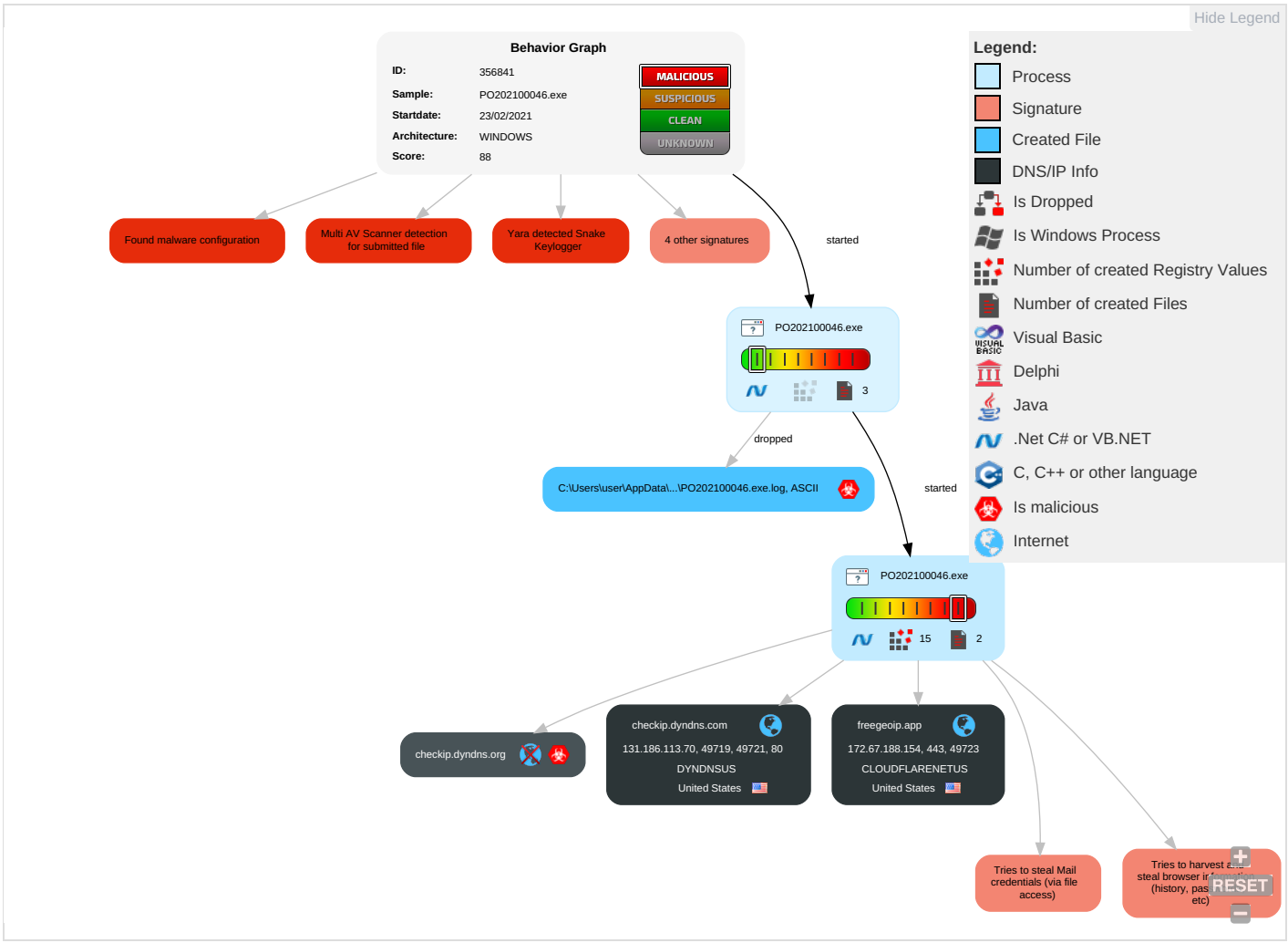


Yara detected Snake Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping 1	Security Software Discovery 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdro Insecure Network Commun
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	Input Capture 1	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Data from Local System 1	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols

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
PO202100046.exe	35%	Virustotal		Browse
PO202100046.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	
PO202100046.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.PO202100046.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File

Domains

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

Copyright null 2021

URLs

Source	Detection	Scanner	Label	Link
http://checkip.dyndns.org4	0%	URL Reputation	safe	
http://checkip.dyndns.org4	0%	URL Reputation	safe	
http://checkip.dyndns.org4	0%	URL Reputation	safe	
http://checkip.dyndns.org4	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/	0%	URL Reputation	safe	
http://checkip.dyndns.org/	0%	Virustotal		Browse
http://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org/HB	0%	Avira URL Cloud	safe	
http://https://freegeoip.app	0%	URL Reputation	safe	
http://https://freegeoip.app	0%	URL Reputation	safe	
http://https://freegeoip.app	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.38	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.38	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.38	0%	URL Reputation	safe	
http://checkip.dyndns.org	0%	Avira URL Cloud	safe	
http://https://freegeoip.app4	0%	URL Reputation	safe	
http://https://freegeoip.app4	0%	URL Reputation	safe	
http://https://freegeoip.app4	0%	URL Reputation	safe	
http://checkip.dyndns.com	0%	Avira URL Cloud	safe	
http://https://freegeoip.app/xml/84.17.52.38x	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.38x	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/84.17.52.38x	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/LoadCountryNameClipboard	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/LoadCountryNameClipboard	0%	URL Reputation	safe	
http://https://freegeoip.app/xml/LoadCountryNameClipboard	0%	URL Reputation	safe	
http://freegeoip.app	0%	URL Reputation	safe	
http://freegeoip.app	0%	URL Reputation	safe	
http://freegeoip.app	0%	URL Reputation	safe	
http://checkip.dyndns.orgD8	0%	URL Reputation	safe	
http://checkip.dyndns.orgD8	0%	URL Reputation	safe	
http://checkip.dyndns.orgD8	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
freegeoip.app	172.67.188.154	true	false	• 0%, Virustotal, Browse	unknown
checkip.dyndns.com	131.186.113.70	true	false	• 0%, Virustotal, Browse	unknown
checkip.dyndns.org	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

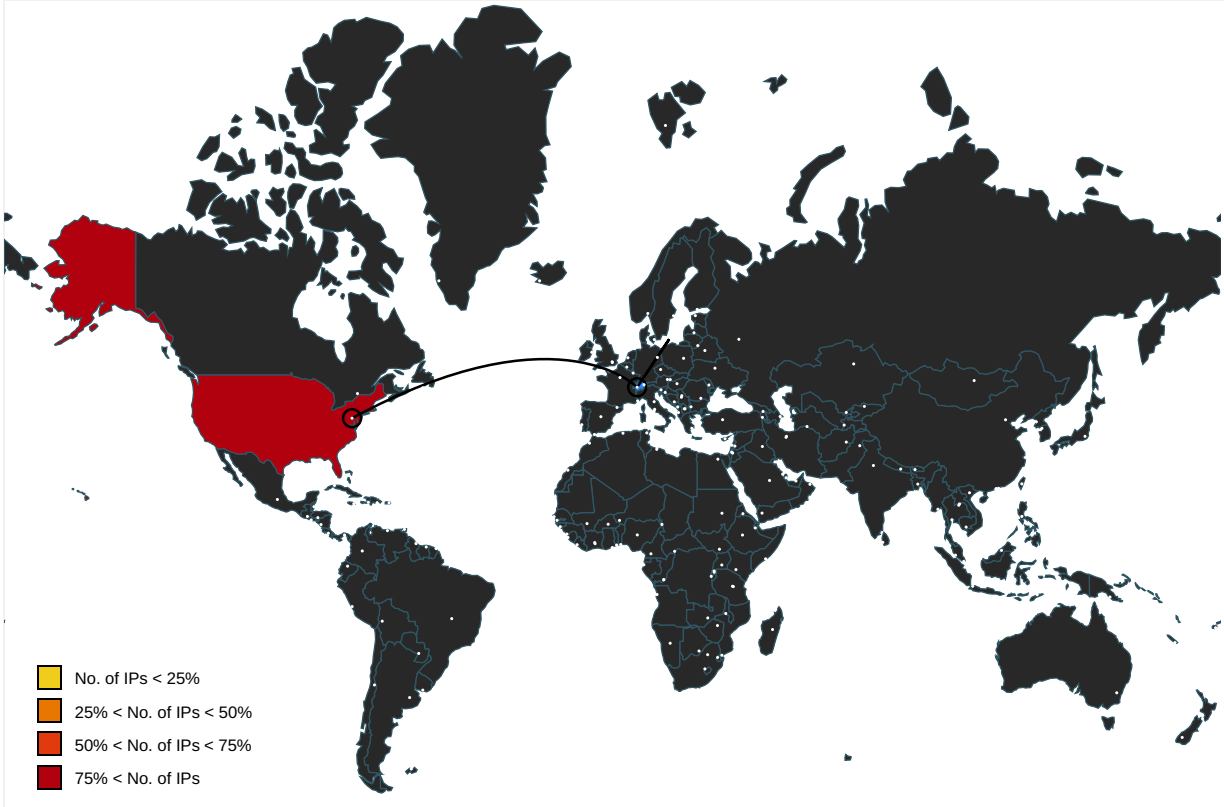
Name	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org4	PO202100046.exe, 00000001.00000002.590354272.0000000002E56000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://freegeoip.app/xml/	PO202100046.exe, 00000001.00000002.590395262.0000000002E66000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/HB	PO202100046.exe, 00000001.00000002.590242317.0000000002DB1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://freegeoip.app	PO202100046.exe, 00000001.00000002.590395262.0000000002E6600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot/sendMessage?chat_id=&text=Createutf-8	PO202100046.exe, 00000001.00000002.590242317.0000000002DB1000.00000004.00000001.sdmp	false		high
http://https://freegeoip.app/xml/84.17.52.38	PO202100046.exe, 00000001.00000002.590395262.0000000002E6600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.org	PO202100046.exe, 00000001.00000002.590395262.0000000002E6600.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://blog.naver.com/cubemit314Ghttp://projectofsonagi.tistory.com/	PO202100046.exe, 00000000.00000002.323967870.000000000348900.00000004.00000001.sdmp	false		high
http://https://freegeoip.app4	PO202100046.exe, 00000001.00000002.590395262.0000000002E6600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.com	PO202100046.exe, 00000001.00000002.590395262.0000000002E6600.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PO202100046.exe, 00000001.00000002.590242317.0000000002DB1000.00000004.00000001.sdmp	false		high
http://https://freegeoip.app/xml/84.17.52.38x	PO202100046.exe, 00000001.00000002.590395262.0000000002E6600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://freegeoip.app/xml/LoadCountryNameClipboard	PO202100046.exe, 00000001.00000002.590242317.0000000002DB1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://freegeoip.app	PO202100046.exe, 00000001.00000002.590395262.0000000002E6600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.orgD8	PO202100046.exe, 00000001.00000002.590395262.0000000002E6600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
131.186.113.70	unknown	United States		33517	DYNDNSUS	false
172.67.188.154	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356841
Start date:	23.02.2021
Start time:	17:40:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO202100046.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
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:	mal88.troj.spyw.evad.winEXE@3/1@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 71% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 52.255.188.83, 168.61.161.212, 23.211.6.115, 104.42.151.234, 51.11.168.160, 8.253.207.120, 8.248.97.254, 8.238.85.126, 8.241.80.126, 8.248.115.254, 51.103.5.186, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194, 184.30.24.56 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
131.186.113.70	P00760000.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Order.doc	Get hash	malicious	Browse	• checkip.dyndns.org/
	purchase order.exe	Get hash	malicious	Browse	• checkip.dyndns.org/

Copyright null 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• checkip.dyndns.org/
	Purchase Order.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	dot crypted.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	v2.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	purchase order.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	9073782912,pdf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Halkbank_Ekstre_20210222_082357_541079.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Order_C3350191107102300.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Payment information 366531890544-2222021,pdf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	RFQ file_pdf.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	cotizaci#U00f3n.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	FOB offer_1164087223_I0133P2100363812.PDF.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	NEW ORDER.19022021.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	orden de compra.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
172.67.188.154	3MndTUzGQn.exe	Get hash	malicious	Browse	• freegeoip.app/json

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
freegeoip.app	SSGLPOJ6212202.exe	Get hash	malicious	Browse	• 104.21.19.200
	ST_PLC URGENT ORDER 0223308737,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	P00760000.exe	Get hash	malicious	Browse	• 104.21.19.200
	Order.doc	Get hash	malicious	Browse	• 104.21.19.200
	QUOTE.doc	Get hash	malicious	Browse	• 104.21.19.200
	Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	purchase order.exe	Get hash	malicious	Browse	• 104.21.19.200
	9073782912,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 104.21.19.200
	Purchase Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	dot crypted.exe	Get hash	malicious	Browse	• 104.21.19.200
	v2.exe	Get hash	malicious	Browse	• 172.67.188.154
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 172.67.188.154
	Halkbank_Ekstre_20210223_082357_541079.exe	Get hash	malicious	Browse	• 172.67.188.154
	FOB offer_1164087223_I0133P2100363812.PDF.exe	Get hash	malicious	Browse	• 104.21.19.200
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 172.67.188.154
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	(appproved)WJO-TT180,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase order.exe	Get hash	malicious	Browse	• 172.67.188.154
	9073782912,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
checkip.dyndns.com	SSGLPOJ6212202.exe	Get hash	malicious	Browse	• 216.146.43.70
	ST_PLC URGENT ORDER 0223308737,pdf.exe	Get hash	malicious	Browse	• 216.146.43.70
	P00760000.exe	Get hash	malicious	Browse	• 162.88.193.70
	Order.doc	Get hash	malicious	Browse	• 131.186.113.70
	QUOTE.doc	Get hash	malicious	Browse	• 216.146.43.70
	Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 162.88.193.70
	purchase order.exe	Get hash	malicious	Browse	• 131.186.113.70
	9073782912,pdf.exe	Get hash	malicious	Browse	• 216.146.43.70

Copyright null 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 131.186.113.70
	Purchase Order.exe	Get hash	malicious	Browse	• 131.186.113.70
	dot crypted.exe	Get hash	malicious	Browse	• 131.186.113.70
	v2.exe	Get hash	malicious	Browse	• 131.186.113.70
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 216.146.43.71
	Halkbank_Ekstre_20210223_082357_541079.exe	Get hash	malicious	Browse	• 162.88.193.70
	FOB offer_1164087223_I0133P2100363812.PDF.exe	Get hash	malicious	Browse	• 162.88.193.70
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 131.186.113.70
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	(appproved)WJO-TT180,pdf.exe	Get hash	malicious	Browse	• 131.186.161.70
	purchase order.exe	Get hash	malicious	Browse	• 131.186.113.70
	9073782912,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DYNDNSUS	SSGLPOJ6212202.exe	Get hash	malicious	Browse	• 216.146.43.71
	ST_PLC URGENT ORDER 0223308737,pdf.exe	Get hash	malicious	Browse	• 216.146.43.70
	P00760000.exe	Get hash	malicious	Browse	• 162.88.193.70
	Order.doc	Get hash	malicious	Browse	• 162.88.193.70
	QUOTE.doc	Get hash	malicious	Browse	• 216.146.43.70
	Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 162.88.193.70
	purchase order.exe	Get hash	malicious	Browse	• 131.186.113.70
	9073782912,pdf.exe	Get hash	malicious	Browse	• 216.146.43.70
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 131.186.113.70
	Purchase Order.exe	Get hash	malicious	Browse	• 131.186.113.70
	dot crypted.exe	Get hash	malicious	Browse	• 131.186.113.70
	v2.exe	Get hash	malicious	Browse	• 131.186.113.70
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 216.146.43.71
	Halkbank_Ekstre_20210223_082357_541079.exe	Get hash	malicious	Browse	• 162.88.193.70
	FOB offer_1164087223_I0133P2100363812.PDF.exe	Get hash	malicious	Browse	• 162.88.193.70
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 131.186.113.70
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
	(appproved)WJO-TT180,pdf.exe	Get hash	malicious	Browse	• 131.186.161.70
	purchase order.exe	Get hash	malicious	Browse	• 131.186.113.70
	9073782912,pdf.exe	Get hash	malicious	Browse	• 131.186.113.70
CLOUDFLARENETUS	SSGLPOJ6212202.exe	Get hash	malicious	Browse	• 172.67.188.154
	ST_PLC URGENT ORDER 0223308737,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	SecuriteInfo.com.Trojan.GenericKD.45695593.9197.exe	Get hash	malicious	Browse	• 172.67.199.58
	SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe	Get hash	malicious	Browse	• 104.23.98.190
	1vuet1S3tI.exe	Get hash	malicious	Browse	• 172.67.199.58
	P00760000.exe	Get hash	malicious	Browse	• 104.21.19.200
	Order.doc	Get hash	malicious	Browse	• 104.21.19.200
	QUOTE.doc	Get hash	malicious	Browse	• 104.21.19.200
	Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	2070121_SN-WS.exe	Get hash	malicious	Browse	• 104.21.71.230
	purchase order.exe	Get hash	malicious	Browse	• 104.21.19.200
	9073782912,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	payment_advice.doc	Get hash	malicious	Browse	• 172.67.172.17
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	dot crypted.exe	Get hash	malicious	Browse	• 104.21.19.200
	New Order 2300030317388 InterMetro.exe	Get hash	malicious	Browse	• 172.67.172.17
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	• 172.67.172.17
	Purchase Order list.exe	Get hash	malicious	Browse	• 104.21.23.61
	RkoKlvuLh6.exe	Get hash	malicious	Browse	• 162.159.136.232

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	SSGLPOJ6212202.exe	Get hash	malicious	Browse	• 172.67.188.154
	ST_PLC URGENT ORDER 0223308737,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	SecuriteInfo.com.Trojan.Siggen12.2497.1023.exe	Get hash	malicious	Browse	• 172.67.188.154

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	P00760000.exe	Get hash	malicious	Browse	• 172.67.188.154
	Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	purchase order.exe	Get hash	malicious	Browse	• 172.67.188.154
	9073782912,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order.exe	Get hash	malicious	Browse	• 172.67.188.154
	dot crypted.exe	Get hash	malicious	Browse	• 172.67.188.154
	v2.exe	Get hash	malicious	Browse	• 172.67.188.154
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 172.67.188.154
	Halkbank_Ekstre_20210223_082357_541079.exe	Get hash	malicious	Browse	• 172.67.188.154
	FOB offer_1164087223_I0133P2100363812.PDF.exe	Get hash	malicious	Browse	• 172.67.188.154
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 172.67.188.154
	Yao Han Industries 61007-51333893QR001U,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	(appproved)WJO-TT180,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	purchase order.exe	Get hash	malicious	Browse	• 172.67.188.154
	9073782912,pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	SOS URGENT RFQ #2345.exe	Get hash	malicious	Browse	• 172.67.188.154
	purchase order 1.exe	Get hash	malicious	Browse	• 172.67.188.154

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO202100046.exe.log

Process:	C:\Users\user\Desktop\PO202100046.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	706
Entropy (8bit):	5.342604339328228
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCq1KDLI4M9tDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKm:MLUE4Kx1qE4qpE4Ks2wKDE4KhK3VZ9px
MD5:	34580C7C598E15B8A008C82FE6A07CDF
SHA1:	2C90E9B7F4AFFE8FC7F9C313B4B867DF5B96CAC1
SHA-256:	08246B9BE1C37F8977CE083319A9D34BE09C65B926CBA30A5E062D79D5A4F1D6
SHA-512:	D836A862804608C3A127BF0CD30ECFB428E682D5E73D90C4C2837F93F02F12307F242F47F3CBBD71249AA6E608AFE230527F2F7D306A35A681346F9DDFE9D820
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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.980014580995005
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:	PO202100046.exe
File size:	614912
MD5:	eafc433b4d4bf4a0edc9b57b6f4af8ec

General

SHA1:	0ba21c1f4f908e589db07ce4003786e0e7bf62d9
SHA256:	77ee17838c1ea6e3c69ec2989df485386800901ef0caac90e01fadbad225a354
SHA512:	ac519009f2d1b9199b3ca37186472a3f138622f063b8465b540d5657258565c4fbf407c9a0188395828ea3a63b48005022eaec7d481b823308e70481b549263c
SSDEEP:	12288:ICbYQjoiur3J9MEQELc5LqbNcyWR4Yem7MX6zDk0OAZnref4:ICbYQjoBr3J9MEQwj63kutr
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!(b.....0..X.....v... .....@.. .....@.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4976de
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xA4622821 [Thu May 24 02:17:05 2057 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9768c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x98000	0x5d6	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x956e4	0x95800	False	0.627196449101	data	7.98391026128	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x98000	0x5d6	0x600	False	0.418619791667	data	4.12696293065	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x980a0	0x34c	data		
RT_MANIFEST	0x983ec	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

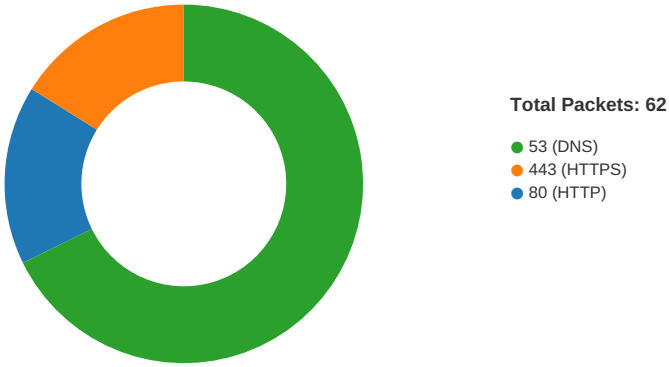
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020
Assembly Version	1.0.0.0
InternalName	ScreenCapturer.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	

Description	Data
Comments	
ProductName	ScreenCapturer
ProductVersion	1.0.0.0
FileDescription	ScreenCapturer
OriginalFilename	ScreenCapturer.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:41:24.970299006 CET	49719	80	192.168.2.6	131.186.113.70
Feb 23, 2021 17:41:25.030709982 CET	80	49719	131.186.113.70	192.168.2.6
Feb 23, 2021 17:41:25.030822039 CET	49719	80	192.168.2.6	131.186.113.70
Feb 23, 2021 17:41:25.031599045 CET	49719	80	192.168.2.6	131.186.113.70
Feb 23, 2021 17:41:25.092823029 CET	80	49719	131.186.113.70	192.168.2.6
Feb 23, 2021 17:41:25.092909098 CET	80	49719	131.186.113.70	192.168.2.6
Feb 23, 2021 17:41:25.092941046 CET	80	49719	131.186.113.70	192.168.2.6
Feb 23, 2021 17:41:25.093041897 CET	49719	80	192.168.2.6	131.186.113.70
Feb 23, 2021 17:41:25.094394922 CET	49719	80	192.168.2.6	131.186.113.70
Feb 23, 2021 17:41:25.154534101 CET	80	49719	131.186.113.70	192.168.2.6
Feb 23, 2021 17:41:25.292853117 CET	49721	80	192.168.2.6	131.186.113.70
Feb 23, 2021 17:41:25.353338957 CET	80	49721	131.186.113.70	192.168.2.6
Feb 23, 2021 17:41:25.354296923 CET	49721	80	192.168.2.6	131.186.113.70
Feb 23, 2021 17:41:25.354636908 CET	49721	80	192.168.2.6	131.186.113.70
Feb 23, 2021 17:41:25.415910006 CET	80	49721	131.186.113.70	192.168.2.6
Feb 23, 2021 17:41:25.528614044 CET	80	49721	131.186.113.70	192.168.2.6
Feb 23, 2021 17:41:25.528637886 CET	80	49721	131.186.113.70	192.168.2.6
Feb 23, 2021 17:41:25.528831005 CET	49721	80	192.168.2.6	131.186.113.70
Feb 23, 2021 17:41:25.530239105 CET	49721	80	192.168.2.6	131.186.113.70
Feb 23, 2021 17:41:25.590226889 CET	80	49721	131.186.113.70	192.168.2.6
Feb 23, 2021 17:41:27.733335018 CET	49723	443	192.168.2.6	172.67.188.154
Feb 23, 2021 17:41:27.786279917 CET	443	49723	172.67.188.154	192.168.2.6
Feb 23, 2021 17:41:27.786389112 CET	49723	443	192.168.2.6	172.67.188.154
Feb 23, 2021 17:41:27.837779999 CET	49723	443	192.168.2.6	172.67.188.154
Feb 23, 2021 17:41:27.890674114 CET	443	49723	172.67.188.154	192.168.2.6
Feb 23, 2021 17:41:27.892535925 CET	443	49723	172.67.188.154	192.168.2.6
Feb 23, 2021 17:41:27.892575026 CET	443	49723	172.67.188.154	192.168.2.6
Feb 23, 2021 17:41:27.892646074 CET	49723	443	192.168.2.6	172.67.188.154
Feb 23, 2021 17:41:27.903217077 CET	49723	443	192.168.2.6	172.67.188.154
Feb 23, 2021 17:41:27.956089020 CET	443	49723	172.67.188.154	192.168.2.6
Feb 23, 2021 17:41:27.956238985 CET	443	49723	172.67.188.154	192.168.2.6

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:41:28.021785021 CET	49723	443	192.168.2.6	172.67.188.154
Feb 23, 2021 17:41:28.255269051 CET	49723	443	192.168.2.6	172.67.188.154
Feb 23, 2021 17:41:28.308166981 CET	443	49723	172.67.188.154	192.168.2.6
Feb 23, 2021 17:41:28.330156088 CET	443	49723	172.67.188.154	192.168.2.6
Feb 23, 2021 17:41:28.521811962 CET	49723	443	192.168.2.6	172.67.188.154
Feb 23, 2021 17:43:08.524080992 CET	49723	443	192.168.2.6	172.67.188.154
Feb 23, 2021 17:43:08.577346087 CET	443	49723	172.67.188.154	192.168.2.6
Feb 23, 2021 17:43:08.577440023 CET	49723	443	192.168.2.6	172.67.188.154

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:41:10.712135077 CET	53	58377	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:11.151542902 CET	55074	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:11.200424910 CET	53	55074	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:11.905694962 CET	54513	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:11.962970972 CET	53	54513	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:12.877499104 CET	62044	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:12.926086903 CET	53	62044	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:13.674206018 CET	63791	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:13.725763083 CET	53	63791	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:14.230628967 CET	64267	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:14.288752079 CET	53	64267	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:14.494139910 CET	49448	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:14.545612097 CET	53	49448	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:15.749825954 CET	60342	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:15.801624060 CET	53	60342	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:16.602288961 CET	61346	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:16.652622938 CET	53	61346	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:17.893213034 CET	51774	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:17.943118095 CET	53	51774	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:19.276487112 CET	56023	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:19.325458050 CET	53	56023	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:20.375060081 CET	58384	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:20.426548958 CET	53	58384	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:21.704137087 CET	60261	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:21.755728960 CET	53	60261	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:22.933409929 CET	56061	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:22.982106924 CET	53	56061	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:23.868319035 CET	58336	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:23.920063019 CET	53	58336	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:24.719208956 CET	53781	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:24.767879009 CET	53	53781	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:24.831747055 CET	54064	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:24.881731987 CET	53	54064	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:25.045636892 CET	52811	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:25.096091986 CET	53	52811	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:26.221689939 CET	55299	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:26.273202896 CET	53	55299	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:27.673002005 CET	63745	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:27.730257988 CET	53	63745	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:28.039052010 CET	50055	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:28.090569973 CET	53	50055	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:29.032175064 CET	61374	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:29.114388943 CET	53	61374	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:30.155915976 CET	50339	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:30.207618952 CET	53	50339	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:31.094937086 CET	63307	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:31.143676043 CET	53	63307	8.8.8.8	192.168.2.6
Feb 23, 2021 17:41:47.499226093 CET	49694	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:41:47.642851114 CET	53	49694	8.8.8.8	192.168.2.6
Feb 23, 2021 17:42:06.983819008 CET	54982	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:42:07.032614946 CET	53	54982	8.8.8.8	192.168.2.6
Feb 23, 2021 17:42:07.442549944 CET	50010	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:42:07.492958069 CET	53	50010	8.8.8.8	192.168.2.6
Feb 23, 2021 17:42:07.678594112 CET	63718	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:42:07.736573935 CET	53	63718	8.8.8.8	192.168.2.6
Feb 23, 2021 17:42:08.597820044 CET	62116	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:42:08.656446934 CET	53	62116	8.8.8.8	192.168.2.6
Feb 23, 2021 17:42:09.287415981 CET	63816	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:42:09.348535061 CET	53	63816	8.8.8.8	192.168.2.6
Feb 23, 2021 17:42:09.798165083 CET	55014	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:42:09.849500895 CET	53	55014	8.8.8.8	192.168.2.6
Feb 23, 2021 17:42:10.096487999 CET	62208	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:42:10.163989067 CET	53	62208	8.8.8.8	192.168.2.6
Feb 23, 2021 17:42:10.489949942 CET	57574	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:42:10.549948931 CET	53	57574	8.8.8.8	192.168.2.6
Feb 23, 2021 17:42:11.117916107 CET	51818	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:42:11.180376053 CET	53	51818	8.8.8.8	192.168.2.6
Feb 23, 2021 17:42:11.790451050 CET	56628	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:42:11.866336107 CET	53	56628	8.8.8.8	192.168.2.6
Feb 23, 2021 17:42:12.751746893 CET	60778	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:42:12.800435066 CET	53	60778	8.8.8.8	192.168.2.6
Feb 23, 2021 17:42:13.731879950 CET	53799	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:42:13.789206982 CET	53	53799	8.8.8.8	192.168.2.6
Feb 23, 2021 17:42:14.282947063 CET	54683	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:42:14.342901945 CET	53	54683	8.8.8.8	192.168.2.6
Feb 23, 2021 17:42:14.473484993 CET	59329	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:42:14.531982899 CET	53	59329	8.8.8.8	192.168.2.6
Feb 23, 2021 17:42:47.109004974 CET	64021	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:42:47.157711983 CET	53	64021	8.8.8.8	192.168.2.6
Feb 23, 2021 17:42:47.523993015 CET	56129	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:42:47.596834898 CET	53	56129	8.8.8.8	192.168.2.6
Feb 23, 2021 17:42:53.807024002 CET	58177	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:42:53.868791103 CET	53	58177	8.8.8.8	192.168.2.6
Feb 23, 2021 17:43:11.126857996 CET	50700	53	192.168.2.6	8.8.8.8
Feb 23, 2021 17:43:11.177244902 CET	53	50700	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 17:41:24.719208956 CET	192.168.2.6	8.8.8.8	0x262	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:41:24.831747055 CET	192.168.2.6	8.8.8.8	0x12df	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Feb 23, 2021 17:41:27.673002005 CET	192.168.2.6	8.8.8.8	0x9156	Standard query (0)	freegeoip.app	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:41:24.767879009 CET	8.8.8.8	192.168.2.6	0x262	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:41:24.767879009 CET	8.8.8.8	192.168.2.6	0x262	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Feb 23, 2021 17:41:24.767879009 CET	8.8.8.8	192.168.2.6	0x262	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Feb 23, 2021 17:41:24.767879009 CET	8.8.8.8	192.168.2.6	0x262	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Feb 23, 2021 17:41:24.767879009 CET	8.8.8.8	192.168.2.6	0x262	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Feb 23, 2021 17:41:24.767879009 CET	8.8.8.8	192.168.2.6	0x262	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Feb 23, 2021 17:41:24.881731987 CET	8.8.8.8	192.168.2.6	0x12df	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)

Copyright null 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:41:24.881731987 CET	8.8.8.8	192.168.2.6	0x12df	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Feb 23, 2021 17:41:24.881731987 CET	8.8.8.8	192.168.2.6	0x12df	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Feb 23, 2021 17:41:24.881731987 CET	8.8.8.8	192.168.2.6	0x12df	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Feb 23, 2021 17:41:24.881731987 CET	8.8.8.8	192.168.2.6	0x12df	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Feb 23, 2021 17:41:24.881731987 CET	8.8.8.8	192.168.2.6	0x12df	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Feb 23, 2021 17:41:27.730257988 CET	8.8.8.8	192.168.2.6	0x9156	No error (0)	freegeoip.app		172.67.188.154	A (IP address)	IN (0x0001)
Feb 23, 2021 17:41:27.730257988 CET	8.8.8.8	192.168.2.6	0x9156	No error (0)	freegeoip.app		104.21.19.200	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- checkip.dyndns.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49719	131.186.113.70	80	C:\Users\user\Desktop\PO202100046.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:41:25.031599045 CET	1156	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
Feb 23, 2021 17:41:25.092909098 CET	1157	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 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 33 38 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: 84.17.52.38</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49721	131.186.113.70	80	C:\Users\user\Desktop\PO202100046.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:41:25.354636908 CET	1158	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
Feb 23, 2021 17:41:25.528614044 CET	1163	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.0.1 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 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 33 38 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: 84.17.52.38</body></html>

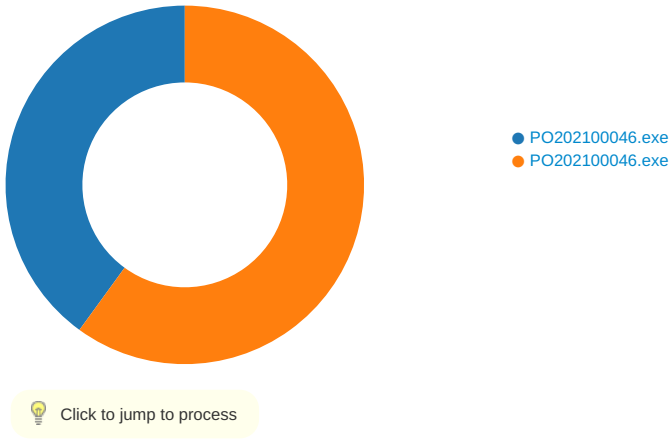
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 17:41:27.892575026 CET	172.67.188.154	443	192.168.2.6	49723	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 10 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Tue Aug 10 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PO202100046.exe PID: 6952 Parent PID: 5848

General

Start time:	17:41:18
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\PO202100046.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO202100046.exe'
Imagebase:	0x40000
File size:	614912 bytes
MD5 hash:	EAFC433B4D4BF4A0EDC9B57B6F4AF8EC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000000.00000002.325194217.0000000004A90000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000000.00000003.319958198.0000000004C71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000003.319958198.0000000004C71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000000.00000002.323967870.0000000003489000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.323967870.0000000003489000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO202100046.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1FC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO202100046.exe.log	unknown	706	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 32 2c 22 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, C	success or wait	1	6E1FC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown

Analysis Process: PO202100046.exe PID: 6988 Parent PID: 6952

General

Start time:	17:41:19
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\PO202100046.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO202100046.exe
Imagebase:	0x8b0000
File size:	614912 bytes
MD5 hash:	EAFC433B4D4BF4A0EDC9B57B6F4AF8EC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000001.00000002.588473253.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000001.00000002.588473253.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\container.dat	success or wait	1	6CD36A95	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies\deprecated.cookie	success or wait	1	6CD36A95	DeleteFileW
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	success or wait	1	6CD36A95	DeleteFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CD31B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis