ID: 344901
Sample Name: PO13132021.scr
Cookbook: default.jbs
Time: 12:32:48
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

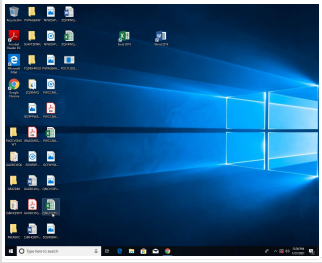
Analysis Report PO13132021.scr

Overview

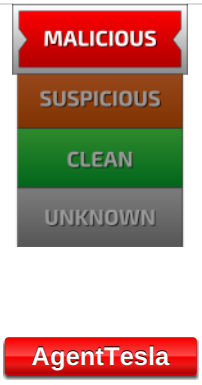
General Information

Sample Name:	PO13132021.scr (renamed file extension from scr to exe)
Analysis ID:	344901
MD5:	7c4c3a12f367dcd..
SHA1:	b0a7b80ddd9b86..
SHA256:	1a1e74fbe89bed3.
Tags:	AgentTesla

Most interesting Screenshot:



Detection



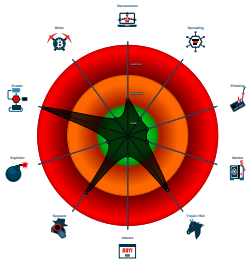
AgentTesla

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

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (creates a PE fi…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Found evasive API chain (trying to d…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Queries sensitive BIOS Information …

Classification



Startup

- **System is w10x64**
- PO13132021.exe (PID: 6960 cmdline: 'C:\Users\user\Desktop\PO13132021.exe' MD5: 7C4C3A12F367DCD154ACCCE5948EBAEB)
  - ioqwel.exe (PID: 6996 cmdline: C:\Users\user\AppData\Local\Temp\Nla\ioqwel.exe C:\Users\user\AppData\Local\Temp\Nla\zfngholtp.s MD5: C56B5F0201A3B3DE53E561FE76912BFD)
    - tpiyon2.exe (PID: 7028 cmdline: C:\Users\user\AppData\Local\Temp\Nla\ioqwel.exe C:\Users\user\AppData\Local\Temp\Nla\zfngholtp.s MD5: 535DD1329AEF11BF4654B3270F026D5B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "q8yz7CCwgQfF",
  "URL: ": "http://8fEo7xWGmGml.org",
  "To: ": "",
  "ByHost: ": "polar.argondns.net:587",
  "Password: ": "dKUidybLVbHYBgI",
  "From: ": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.587931278.0000000003E01000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.213456226.00000000032F0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.583608219.0000000000CA6000.00000004.00000020.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.582750259.0000000000400000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.583897205.0000000002812000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 7 entries				

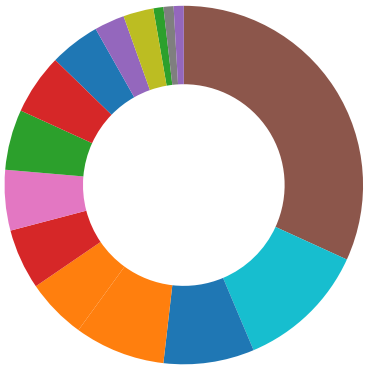
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.tpiyon2.exe.2810000.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.ioqwel.exe.32f0000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.tpiyon2.exe.27d0000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.1.tpiyon2.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.tpiyon2.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Detected unpacking (creates a PE file in dynamic memory)

Detected unpacking (overwrites its own PE header)

Uses 32bit PE files

Uses new MSVCR Dlls

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

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (creates a PE file in dynamic memory)

Detected unpacking (overwrites its own PE header)

Malware Analysis System Evasion:

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

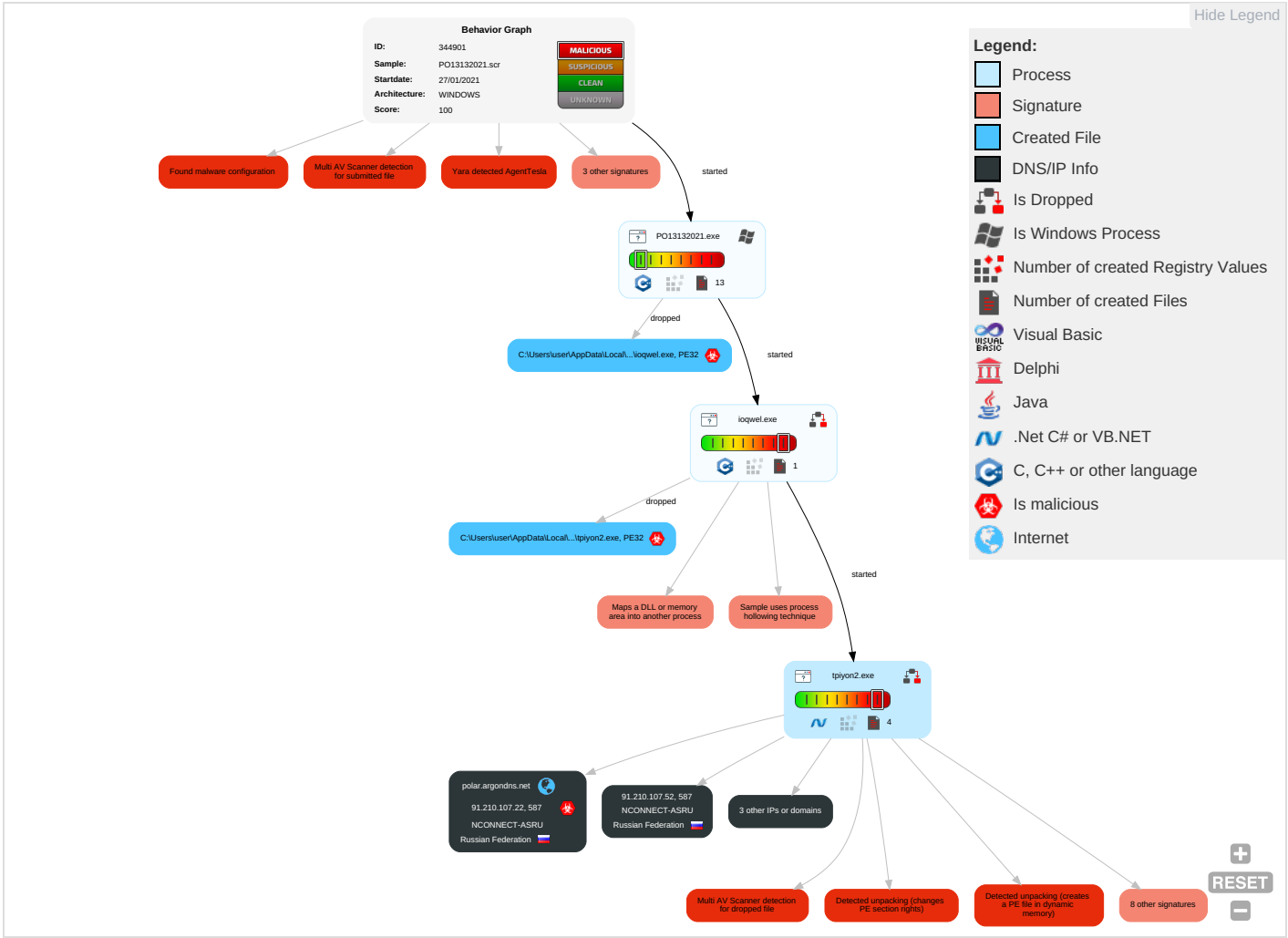
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Valid Accounts 2	Windows Management Instrumentation 2 1 1	Valid Accounts 2	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypte Channel
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Valid Accounts 2	Deobfuscate/Decode Files or Information 1 1	Input Capture 2 1	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Star Port 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Access Token Manipulation 2 1	Obfuscated Files or Information 2	Credentials in Registry 1	System Information Discovery 1 2 8	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-App Layer Pr
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 2 1 2	Software Packing 3 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer	Applicati Protocol
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Valid Accounts 2	LSA Secrets	Security Software Discovery 2 5 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiban Commun
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 2 1	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Common Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 2 1 2	Proc Filesystem	Application Window Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicati Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pro

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
PO13132021.exe	27%	Virustotal		Browse
PO13132021.exe	28%	ReversingLabs	Win32.Trojan.Generic	
PO13132021.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Nla\ioqwel.exe	5%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Nla\ioqwel.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\Nla\tpiyon2.exe	21%	ReversingLabs	Win32.PUA.Wacapew	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.tpiyon2.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.1.tpiyon2.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.PO13132021.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.2.tpiyon2.exe.2810000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.0.PO13132021.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Domains

Source	Detection	Scanner	Label	Link
polar.argondns.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://8fEo7xWGmGml.org	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://zztVNZ.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
polar.argondns.net	91.210.107.22	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

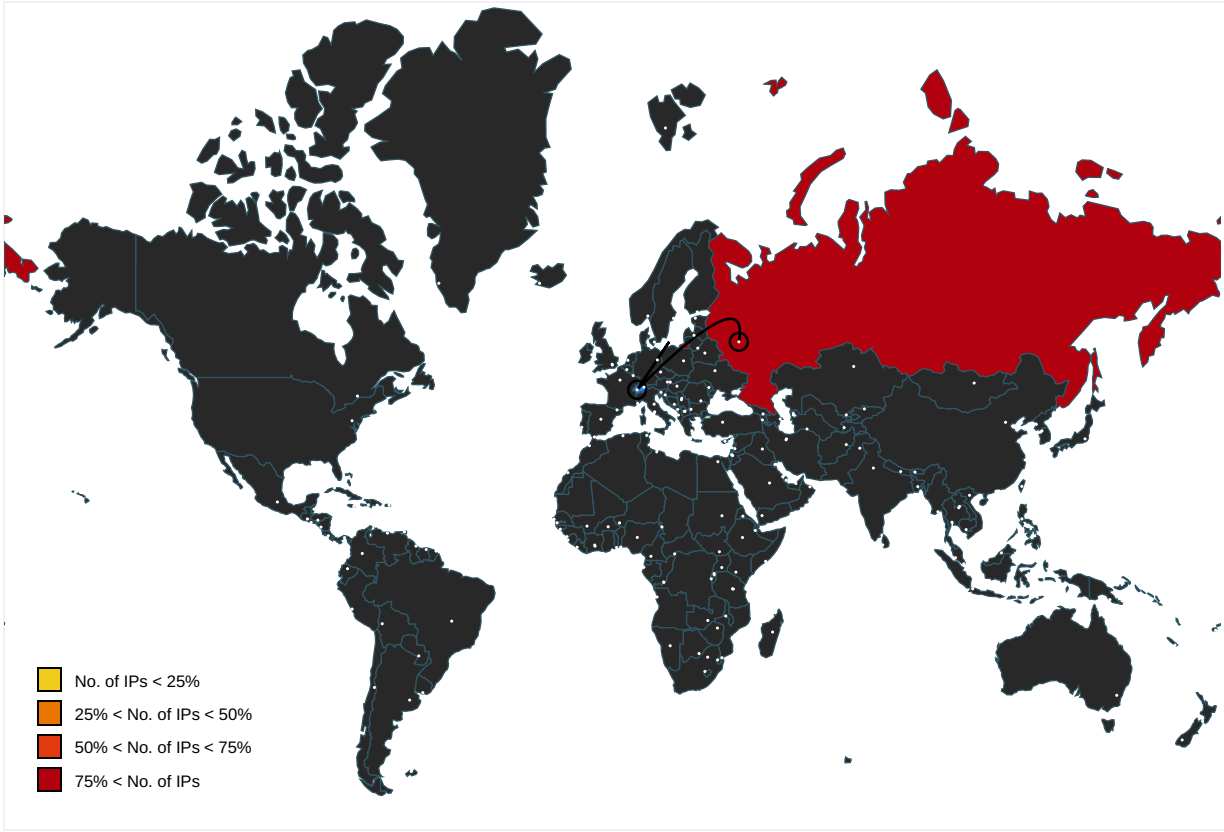
Name	Malicious	Antivirus Detection	Reputation
http://8fEo7xWGmGml.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	PO13132021.exe, 00000000.00000002.217235174.00000000028E0000.00000004.00000001.sdmp, ioqwel.exe, 00000001.00000000.202042794.0000000000B79000.00000002.00020000.sdmp, tpiyon2.exe, 00000002.00000000.205351945.00000000004C9000.00000002.00020000.sdmp, ioqwel.exe.0.dr	false		high
http://127.0.0.1:HTTP/1.1	tpiyon2.exe, 00000002.00000002.586869289.0000000002E01000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	tpiyon2.exe, 00000002.00000002.586869289.0000000002E01000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_Error	PO13132021.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	PO13132021.exe	false		high
http://https://www.autoitscript.com/autoit3/	PO13132021.exe, 00000000.00000002.217235174.00000000028E0000.00000004.00000001.sdmp, ioqwel.exe, 00000001.00000002.214822872.00000000004553000.00000004.00000001.sdmp, ioqwel.exe.0.dr	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	tpiyon2.exe, 00000002.00000002.586869289.0000000002E01000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://zztVNZ.com	tpiyon2.exe, 00000002.00000002.586869289.0000000002E01000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	ioqwel.exe, 00000001.00000002.213456226.00000000032F0000.00000004.00000001.sdmp, tpiyon2.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.210.107.22	unknown	Russian Federation		49335	NCONNECT-ASRU	true
91.210.107.54	unknown	Russian Federation		49335	NCONNECT-ASRU	false
91.210.107.62	unknown	Russian Federation		49335	NCONNECT-ASRU	false
91.210.107.53	unknown	Russian Federation		49335	NCONNECT-ASRU	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.210.107.52	unknown	Russian Federation		49335	NCONNECT-ASRU	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344901
Start date:	27.01.2021
Start time:	12:32:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO13132021.scr (renamed file extension from scr to 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:	mal100.troj.spyw.evad.winEXE@5/5@1/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 26.5% (good quality ratio 24.8%) • Quality average: 79.3% • Quality standard deviation: 29.6%
HCA Information:	• Successful, ratio: 58% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 51.11.168.160, 23.210.248.85, 20.54.26.129, 95.101.27.142, 95.101.27.163, 51.103.5.186, 95.101.22.216, 95.101.22.224, 51.104.139.180, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:33:46	API Interceptor	1017x Sleep call for process: tpiyon2.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.210.107.22	haitianx.exe	Get hash	malicious	Browse	
	pPKwe2k3h8.exe	Get hash	malicious	Browse	
	POn#U00b0 08312020xlx.exe	Get hash	malicious	Browse	
91.210.107.54	haitianx.exe	Get hash	malicious	Browse	
	pPKwe2k3h8.exe	Get hash	malicious	Browse	
91.210.107.62	haitianx.exe	Get hash	malicious	Browse	
91.210.107.53	haitianx.exe	Get hash	malicious	Browse	
	pPKwe2k3h8.exe	Get hash	malicious	Browse	
	New Order Feb.,2021.doc	Get hash	malicious	Browse	
91.210.107.52	nFEmhKJpQ3.exe	Get hash	malicious	Browse	
	wamoH1JlFE.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
polar.argondns.net	haitianx.exe	Get hash	malicious	Browse	• 91.210.107.22
	pPKwe2k3h8.exe	Get hash	malicious	Browse	• 91.210.107.22
	New Order Feb.,2021.doc	Get hash	malicious	Browse	• 91.210.107.62
	nFEmhKJpQ3.exe	Get hash	malicious	Browse	• 91.210.107.52
	wamoH1JlFE.exe	Get hash	malicious	Browse	• 91.210.107.52
	POn#U00b0 08312020xlx.exe	Get hash	malicious	Browse	• 91.210.107.22

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NCONNECT-ASRU	haitianx.exe	Get hash	malicious	Browse	• 91.210.107.53
	pPKwe2k3h8.exe	Get hash	malicious	Browse	• 91.210.107.53
	New Order Feb.,2021.doc	Get hash	malicious	Browse	• 91.210.107.53
	nFEmhKJpQ3.exe	Get hash	malicious	Browse	• 91.210.107.52
	wamoH1JlFE.exe	Get hash	malicious	Browse	• 91.210.107.52
	2019-06-12-malware-EXE-from-80.85.155.70.exe	Get hash	malicious	Browse	• 80.85.155.70
	Ca4fOzoNzJ.exe	Get hash	malicious	Browse	• 94.177.123.237
	elOHMq4FF0.exe	Get hash	malicious	Browse	• 94.177.123.237
	z4Bx3C0Q50.exe	Get hash	malicious	Browse	• 94.177.123.237
	SecuriteInfo.com.Downloader-FBZCB076D449C2FA.exe	Get hash	malicious	Browse	• 94.177.123.237
	SecuriteInfo.com.ArtemisE88E9DC9AD1C.exe	Get hash	malicious	Browse	• 185.70.107.72
	o2TVmUuQ2r.exe	Get hash	malicious	Browse	• 185.70.107.73
	Zh3jpW08zI.exe	Get hash	malicious	Browse	• 185.70.107.40
	OKtLV4rzIP.exe	Get hash	malicious	Browse	• 185.70.107.72
	3L42ZG9T7d.exe	Get hash	malicious	Browse	• 185.70.107.35
	http://www.datacentervision.com/	Get hash	malicious	Browse	• 185.130.215.154
	osi.exe	Get hash	malicious	Browse	• 158.255.6.242
	qXpkpxFw.exe	Get hash	malicious	Browse	• 141.105.68.106
	1nk3VTFB.exe	Get hash	malicious	Browse	• 141.105.68.106
	W2WcN9LK.exe	Get hash	malicious	Browse	• 141.105.68.106
NCONNECT-ASRU	haitianx.exe	Get hash	malicious	Browse	• 91.210.107.53
	pPKwe2k3h8.exe	Get hash	malicious	Browse	• 91.210.107.53
	New Order Feb.,2021.doc	Get hash	malicious	Browse	• 91.210.107.53
	nFEmhKJpQ3.exe	Get hash	malicious	Browse	• 91.210.107.52
	wamoH1JlFE.exe	Get hash	malicious	Browse	• 91.210.107.52
	2019-06-12-malware-EXE-from-80.85.155.70.exe	Get hash	malicious	Browse	• 80.85.155.70
	Ca4fOzoNzJ.exe	Get hash	malicious	Browse	• 94.177.123.237
	elOHMq4FF0.exe	Get hash	malicious	Browse	• 94.177.123.237
	z4Bx3C0Q50.exe	Get hash	malicious	Browse	• 94.177.123.237
	SecuriteInfo.com.Downloader-FBZCB076D449C2FA.exe	Get hash	malicious	Browse	• 94.177.123.237
	SecuriteInfo.com.ArtemisE88E9DC9AD1C.exe	Get hash	malicious	Browse	• 185.70.107.72
	o2TVmUuQ2r.exe	Get hash	malicious	Browse	• 185.70.107.73
	Zh3jpW08zI.exe	Get hash	malicious	Browse	• 185.70.107.40
	OKtLV4rzIP.exe	Get hash	malicious	Browse	• 185.70.107.72
	3L42ZG9T7d.exe	Get hash	malicious	Browse	• 185.70.107.35
	http://www.datacentervision.com/	Get hash	malicious	Browse	• 185.130.215.154
	osi.exe	Get hash	malicious	Browse	• 158.255.6.242
	qXpkpxFw.exe	Get hash	malicious	Browse	• 141.105.68.106
	1nk3VTFB.exe	Get hash	malicious	Browse	• 141.105.68.106
	W2WcN9LK.exe	Get hash	malicious	Browse	• 141.105.68.106
NCONNECT-ASRU	haitianx.exe	Get hash	malicious	Browse	• 91.210.107.53
	pPKwe2k3h8.exe	Get hash	malicious	Browse	• 91.210.107.53
	New Order Feb.,2021.doc	Get hash	malicious	Browse	• 91.210.107.53
	nFEmhKJpQ3.exe	Get hash	malicious	Browse	• 91.210.107.52
	wamoH1JlFE.exe	Get hash	malicious	Browse	• 91.210.107.52
	2019-06-12-malware-EXE-from-80.85.155.70.exe	Get hash	malicious	Browse	• 80.85.155.70
	Ca4fOzoNzJ.exe	Get hash	malicious	Browse	• 94.177.123.237
	elOHMq4FF0.exe	Get hash	malicious	Browse	• 94.177.123.237
	z4Bx3C0Q50.exe	Get hash	malicious	Browse	• 94.177.123.237
	SecuriteInfo.com.Downloader-FBZCB076D449C2FA.exe	Get hash	malicious	Browse	• 94.177.123.237
	SecuriteInfo.com.ArtemisE88E9DC9AD1C.exe	Get hash	malicious	Browse	• 185.70.107.72
	o2TVmUuQ2r.exe	Get hash	malicious	Browse	• 185.70.107.73

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Zh3jpW08zI.exe	Get hash	malicious	Browse	• 185.70.107.40
	OKtLV4rzIP.exe	Get hash	malicious	Browse	• 185.70.107.72
	3L42ZG9T7d.exe	Get hash	malicious	Browse	• 185.70.107.35
	http://www.datacentervision.com/	Get hash	malicious	Browse	• 185.130.215.154
	osi.exe	Get hash	malicious	Browse	• 158.255.6.242
	qXpkpxFw.exe	Get hash	malicious	Browse	• 141.105.68.106
	1nk3VTFB.exe	Get hash	malicious	Browse	• 141.105.68.106
	W2WcN9LK.exe	Get hash	malicious	Browse	• 141.105.68.106

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\Nla\ioqwel.exe	Tender documents_FOB_Offer_Printout.PDF.exe	Get hash	malicious	Browse	
	HTG-9087650.exe	Get hash	malicious	Browse	
	Order-0S94442VD VictoryJSC.xlsx	Get hash	malicious	Browse	
	Purchase Order.xlsx	Get hash	malicious	Browse	
	PO#21010028 - SYINDAC QT-00820_pdf.exe	Get hash	malicious	Browse	
	MC8ZX01sSo.exe	Get hash	malicious	Browse	
	F6AAdCq3uj.exe	Get hash	malicious	Browse	
	tZy7EYc9Da.exe	Get hash	malicious	Browse	
	YMQ6XNETnU.exe	Get hash	malicious	Browse	
	AWB 9899691012 TRACKING INFO_pdf.exe	Get hash	malicious	Browse	
	BANK FORM.xlsx	Get hash	malicious	Browse	
	order0004345.xlsx	Get hash	malicious	Browse	
	Bill of Lading BL.xlsx	Get hash	malicious	Browse	
	Clntnjk.xlsx	Get hash	malicious	Browse	
	HTG-9066543.exe	Get hash	malicious	Browse	
	vbc.exe	Get hash	malicious	Browse	
	HTMY-209871640.exe	Get hash	malicious	Browse	
	YOeg64zDX4.exe	Get hash	malicious	Browse	
	qZtylTGU0c.exe	Get hash	malicious	Browse	
	w2kN50kQQ4.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\Nla\tpiyon2.exe	HTG-9087650.exe	Get hash	malicious	Browse	
	Order-0S94442VD VictoryJSC.xlsx	Get hash	malicious	Browse	
	Purchase Order.xlsx	Get hash	malicious	Browse	
	PO#21010028 - SYINDAC QT-00820_pdf.exe	Get hash	malicious	Browse	
	MC8ZX01sSo.exe	Get hash	malicious	Browse	
	F6AAdCq3uj.exe	Get hash	malicious	Browse	
	AWB 9899691012 TRACKING INFO_pdf.exe	Get hash	malicious	Browse	
	HTG-9066543.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\Nla\ioqwel.exe

Process:	C:\Users\user\Desktop\PO13132021.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	893608
Entropy (8bit):	6.620131693023677
Encrypted:	false
SSDEEP:	12288:6pVWeOV7GtlNsegA/hMyyzlcqikvAfcN9b2MyZa31twoPTdFxgawV2M01:6T3E53Myyzl0hMf1tr7Caw8M01
MD5:	C56B5F0201A3B3DE53E561FE76912BFD
SHA1:	2A4062E10A5DE813F5688221DBEB3F3FF33EB417
SHA-256:	237D1BCA6E056DF5BB16A1216A434634109478F882D3B1D58344C801D184F95D
SHA-512:	195B98245BB820085AE9203CDB6D470B749D1F228908093E8606453B027B7D7681CCD7952E30C2F5DD40F8F0B999CCFC60EBB03419B574C08DE6816E75710D2C
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\Nla\ioqwel.exe

Antivirus:	• Antivirus: Metadefender, Detection: 5%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Tender documents_FOB_Offer_Printout.PDF.exe, Detection: malicious, Browse • Filename: HTG-9087650.exe, Detection: malicious, Browse • Filename: Order-0S94442VD VictoryJSC.xlsx, Detection: malicious, Browse • Filename: Purchase Order.xlsx, Detection: malicious, Browse • Filename: PO#21010028 - SYINDAC QT-00820_pdf.exe, Detection: malicious, Browse • Filename: MC8ZX01sSo.exe, Detection: malicious, Browse • Filename: F6AAdCq3uj.exe, Detection: malicious, Browse • Filename: tZy7EYc9Da.exe, Detection: malicious, Browse • Filename: YMQ6XNETnU.exe, Detection: malicious, Browse • Filename: AWB 9899691012 TRACKING INFO_pdf.exe, Detection: malicious, Browse • Filename: BANK FORM.xlsx, Detection: malicious, Browse • Filename: order0004345.xlsx, Detection: malicious, Browse • Filename: Bill of Lading BL.xlsx, Detection: malicious, Browse • Filename: Clntnjk.xlsx, Detection: malicious, Browse • Filename: HTG-9066543.exe, Detection: malicious, Browse • Filename: vbc.exe, Detection: malicious, Browse • Filename: HTMY-209871640.exe, Detection: malicious, Browse • Filename: YOeg64zDX4.exe, Detection: malicious, Browse • Filename: qZtylTGU0c.exe, Detection: malicious, Browse • Filename: w2kN50kQQ4.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sD.R.*.R.*.R.*..C..P.*....S.*._@..a.*._@....*._@..g.*.[j..[.*.[j..w.*.R .+.r.*.....*....S.*._@..S.*.R...P.*....S.*.RichR.*.....PE..L....q.Z....."....@.....@...@.....@.....|.....P..... .....p...q...;..... [..@.....text..... ..`.rdata.....@..@.data...t.....R.....@....rsrc...P.....<.... .....@..@.reloc...q...p...r.....@..B..... .....

C:\Users\user\AppData\Local\Temp\Nla\jsgwugqwc.ftb

Process:	C:\Users\user\Desktop\PO13132021.exe
File Type:	data
Category:	dropped
Size (bytes):	291840
Entropy (8bit):	**7.999300065062373**
Encrypted:	**true**
SSDEEP:	6144:kIFKOy7s3oaqBaQu90yiRK6TRjM9n0z+QfDZnd9R/kBMnF6ZbIfWwxHAz:MP7s3zqc54Kv0zbdnd9eBMnFi6/m
MD5:	E2805AA2B24333EA055CB4524255CCDD
SHA1:	58715C4C2B07B940B8EF975EB4ABCCA218B7882B
SHA-256:	6508B1408DB51A4C59210FDEE7703D284A675460185A3BA70E060F890D7C2EA0
SHA-512:	C6BFE4EF983EA000FC9E9A6E6B0EAC43A1D52C2648FCC68B6DC07A3F0F6CB24D61FAC116D4ACEC76C876EAD47ED97B64D3F03BC3DC7A044F6C319314C139D6D
Malicious:	false
Reputation:	low
Preview:	._...&wBnu.K.^7..K....Cg@.x...Y[.S..|...W.....sZ.!-p.&...).....&...n.4l...s\....bz"..]]./.F.@:6J.+..o|..lD...f..tn./..q.../..0..<.#b.u..D.....~i._.i.m...%O..h.....:.]6`._0..f)./..;.....&.K.".;.u. ..K...P....:...(f....-...y..7M.3...A9.w...D.,S.5..x.2...s....|..&4h&...~..a..;..R.N.5.]xM.K.[.....R.{.....N..g..[.AN}..i..p.....'..R....L.YB.#.Y...w1.P".....2..."a..A. .....<md..<TW..;.... 8..!..... .gbi-E`QW.J...$...H..~....Z.....s+v..z.8..Z...f.A..w.O..G.gn..fs.,.dGD...CU.....gw{../.c $'..#.x]z..l....A...Qq.rO3.C....T\...Zzr..D%.<.G3...d.....,UH.'w!..../..V. .....*...E..RU.n\|h ....G..\.....?.X.v.U....7'*....^~..H/..K.Kv+g.U._....7...M.\,....k.i..[....u(e.k.z.J..'}.l..u._.F.b.a.w`G<@.&u.....z..p..Nc.T..5.2...6?..e.e....L...w..d...FVEx4#h.oK....!RI..6\|....u>..... <CP..zgj..52zI..^..H+.E..%{...j).....IS.hd.b2.F,...\|....{..%'.H.}..T}aqYf&.....}Y..8\|..^?.....$NlX.....t. ...XS..i...b._.d|.1S.. w..3...9..'s..C....c0._MU.d.....j

C:\Users\user\AppData\Local\Temp\Nla\tpiyon2.exe

Process:	C:\Users\user\AppData\Local\Temp\Nla\ioqwel.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	893608
Entropy (8bit):	6.570843086702839
Encrypted:	false
SSDEEP:	12288:apVWeOV7GtlNsegA/hMyyzlcqikvAfcN9b2MyZa31twoPTdFxgawV2M0:aT3E53Myyzl0hMf1tr7Caw8M0
MD5:	535DD1329AEF11BF4654B3270F026D5B
SHA1:	9C84DE0BDE8333F852120AB40710545B3F799300
SHA-256:	B31445FC4B8803D1B7122A6563002CFE3E925FFD1FDC9B84FBA6FC78F6A8B955
SHA-512:	A552E20A09A796A6E3E18DECE308880069C958CF9136BB4FC3EE726D6BC9B2F8EDDBCFF06FF9F9DED4DD268F5D0F39D516AD42ECCE6455A4BF5CF4F3CB4CECC
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 21%

C:\Users\user\AppData\Local\Temp\Nla\tpiyon2.exe	
Joe Sandbox View:	• Filename: HTG-9087650.exe, Detection: malicious, Browse • Filename: Order-0S94442VD VictoryJSC.xlsx, Detection: malicious, Browse • Filename: Purchase Order.xlsx, Detection: malicious, Browse • Filename: PO#21010028 - SYINDAC QT-00820_pdf.exe, Detection: malicious, Browse • Filename: MC8ZX01sSo.exe, Detection: malicious, Browse • Filename: F6AAdCq3uj.exe, Detection: malicious, Browse • Filename: AWB 9899691012 TRACKING INFO_pdf.exe, Detection: malicious, Browse • Filename: HTG-9066543.exe, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....sD.R.*.R.*.R.*..C..P.*....S.*._@..a.*._@....*._@..g.*.[j..[.*.[j..w.*.R .+.r.*.....*....S.*._@..S.*.R...P.*....S.*.RichR.*.....PE..L....q.Z.....@.....@.....@.....@.....@.....|.....P..... .....p...q...;..... [..@.....text..... ..`.rdata.....@..@.data...t.....R.....@....rsrc...P.....<.... .....@..@.reloc...q...p...r.....@..B..... .....

C:\Users\user\AppData\Local\Temp\Nla\zfngholtp.s	
Process:	C:\Users\user\Desktop\PO13132021.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	385136
Entropy (8bit):	4.040875529182386
Encrypted:	false
SSDEEP:	96:D6fyJOogeGFlIvMxquc9JH71Qu1SqETSCmQG5mqpUJguXNR2022OdOQqOxFx7IRU:D6fggwMAuKpWIJB
MD5:	2FF4031E23DF3BA8CA445C0CC35B472C
SHA1:	97AB1DA04AB0A6DA94207C0B6BBF453520A6E615
SHA-256:	F2208559DB506C7F145B43755C42D4F57118A0E26CE9FC5ED60AFFE05066BFC9
SHA-512:	2E675BC7838F47ABC2F3A3E3B28E49A2F7CAD449550B18EE2132503F19AE9CA6E6B6AE9EF0BA7568D03F4032BB15DE9049D97204A6B831CA730E9A31C684071E
Malicious:	false
Reputation:	low
Preview:	Global $Z3232ddy8i5i = Execute("Chr")..#NoTrayIcon..Global $R308k3t564c, $T31p8e, $X32o2tny2y, $A33y7teo, $l34iii, $N353fv6..For $R308k3t564c = 0 To Random(5, 8, 1).. $X32o2tny2y = 0.. For $A33y7teo = 2 To 100.. $T31p8e = True.. $l34iii = 2.. While $l34iii*$l34iii<=$R308k3t564c.. If Mod($R308k3t564c, $l34iii) == 0 Then.. $X32o2tny2y = False.. ExitLoop.. EndIf.. $l34iii += 1.. WEnd.. If $T31p8e Then $X32o2tny2y = $A33y7teo.. Next..Next..Dim $D3231lmvqm = GUICreate($Z3232ddy8i5i((-402+481))&$Z3232ddy8i5i((-364+481))&$Z3232ddy8i5i((-365+481))&$Z3232ddy8i5i((-383+481))&$Z3232ddy8i5i((-364+481))&$Z3232ddy8i5i((-382+481))&$Z3232ddy8i5i((-374+481))&$Z3232ddy8i5i((-449+481))&$Z3232ddy8i5i((-408+481))&$Z3232ddy8i5i((-371+481))&$Z3232ddy8i5i((-382+481)), 102, 240, -99999, -99999, 0, 128)....GUISetState(@SW_SHOW)..Global $C3333m4s7zv2 = Execute($Z3232ddy8i5i((-412+481))&$Z3232ddy8i5i((-361+481))&$Z3232ddy8i5i((-380+481))&$Z3232ddy8i5i((-382+481))&$Z3232ddy8i5i((-364+481))&$Z3232d

C:\Users\user\AppData\Local\Temp\nstBE20.tmp	
Process:	C:\Users\user\Desktop\PO13132021.exe
File Type:	data
Category:	dropped
Size (bytes):	1573047
Entropy (8bit):	6.999007197019042
Encrypted:	false
SSDEEP:	24576:aT3E53Myyzl0hMf1tr7Caw8M0TgDFczdT/m:43EZpBh211Waw30TgDFcBC
MD5:	C1DB9615BCC91F1C6F24F23CE98704BF
SHA1:	AF374C57B8B9D416FAEFA381B4B99D677FB77150
SHA-256:	8AEDAE19F4A93BBA5822454BC6B06CF2D4650FA44B842DA9EEEBD6DF5B4F7DC3
SHA-512:	DE3D0832ACCF2A8582709D02C37DEAF25A7ED29CBAC29A841CB5965A8AF1C50E115A38FF1C8902D037DE50106463A13AE4EA2F531468BDF8CB7C9377A50178D
Malicious:	false
Reputation:	low
Preview:	.....J.....1...g.....j.....N.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.98445424363155

General

TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	PO13132021.exe
File size:	725929
MD5:	7c4c3a12f367dcd154accce5948ebaeb
SHA1:	b0a7b80ddd9b86a20d3a41e3423cedb341b6220c
SHA256:	1a1e74fbe89bed37913351432c163e204018655e51811a abb9e5fc6a06cf5887
SHA512:	3309ff4fa38aca1d791683f80de67ed2ab720dab034dcb9 97e9985623eb57f350959ea2ae5bd542f118b703793630a 6002b38356716819ef9c28b0ce704dc5a4
SSDEEP:	12288:cqOdWKrdSUiJruF2ahX/gjTCSxJMbAbYTqLqPq xG9sCQPb45Yxsy:cZYA2W2QX/cTfw0sTOq/9sPbLxsy
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L.....$_.....d.....a4.....@

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x403461
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D6E4 [Sat Aug 1 02:43:48 2020 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:	ea4e67a31ace1a72683a99b80cf37830

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A130h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B0h]
call dword ptr [004080C0h]
and eax, BFFFFFFFh
cmp ax, 00000006h

Instruction
mov dword ptr [0042474Ch], eax
je 00007F1FC9279883h
push ebx
call 00007F1FC927C9FEh
cmp eax, ebx
je 00007F1FC9279879h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007F1FC927C97Ah
push esi
call dword ptr [004080B8h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F1FC927985Dh
push 0000000Bh
call 00007F1FC927C9D2h
push 00000009h
call 00007F1FC927C9CBh
push 00000007h
mov dword ptr [00424744h], eax
call 00007F1FC927C9BFh
cmp eax, ebx
je 00007F1FC9279881h
push 0000001Eh
call eax
test eax, eax
je 00007F1FC9279879h
or byte ptr [0042474Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [00424818h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0041FD10h
call dword ptr [0040816Ch]
push 0040A1ECh

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8438	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2d000	0x6bc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x8000	0x29c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x623c	0x6400	False	0.65859375	data	6.40257705324	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1274	0x1400	False	0.43359375	data	5.05749598324	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x1a858	0x600	False	0.445963541667	data	4.08975001509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2d000	0x6bc	0x800	False	0.41259765625	data	4.23827605847	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x2d100	0x100	data	English	United States
RT_DIALOG	0x2d200	0x11c	data	English	United States
RT_DIALOG	0x2d31c	0x60	data	English	United States
RT_MANIFEST	0x2d37c	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

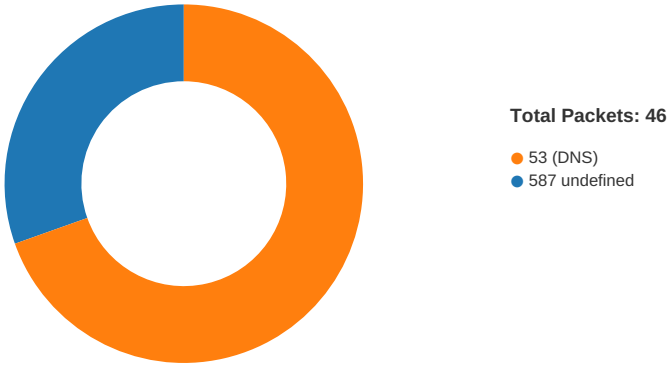
DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, GetTempFileNameA, RemoveDirectoryA, WriteFile, CreateDirectoryA, GetLastError, CreateProcessA, GlobalLock, GlobalUnlock, CreateThread, lstrcpynA, SetErrorMode, GetDiskFreeSpaceA, lstrlenA, GetCommandLineA, GetVersion, GetWindowsDirectoryA, SetEnvironmentVariableA, GetTempPathA, CopyFileA, GetCurrentProcess, ExitProcess, GetModuleFileNameA, GetFileSize, ReadFile, GetTickCount, Sleep, CreateFileA, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 12:35:08.558293104 CET	49743	587	192.168.2.3	91.210.107.22
Jan 27, 2021 12:35:11.559736013 CET	49743	587	192.168.2.3	91.210.107.22
Jan 27, 2021 12:35:17.591324091 CET	49743	587	192.168.2.3	91.210.107.22
Jan 27, 2021 12:35:29.609376907 CET	49743	587	192.168.2.3	91.210.107.62
Jan 27, 2021 12:35:32.624046087 CET	49743	587	192.168.2.3	91.210.107.62
Jan 27, 2021 12:35:38.640366077 CET	49743	587	192.168.2.3	91.210.107.62
Jan 27, 2021 12:35:50.657453060 CET	49743	587	192.168.2.3	91.210.107.53
Jan 27, 2021 12:35:53.656806946 CET	49743	587	192.168.2.3	91.210.107.53
Jan 27, 2021 12:35:59.673070908 CET	49743	587	192.168.2.3	91.210.107.53
Jan 27, 2021 12:36:11.731405973 CET	49743	587	192.168.2.3	91.210.107.54
Jan 27, 2021 12:36:14.736784935 CET	49743	587	192.168.2.3	91.210.107.54
Jan 27, 2021 12:36:20.745368004 CET	49743	587	192.168.2.3	91.210.107.54
Jan 27, 2021 12:36:32.758579016 CET	49743	587	192.168.2.3	91.210.107.52
Jan 27, 2021 12:36:35.774386883 CET	49743	587	192.168.2.3	91.210.107.52

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 12:33:30.401842117 CET	58361	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:33:30.450095892 CET	53	58361	8.8.8.8	192.168.2.3
Jan 27, 2021 12:33:31.753947973 CET	63492	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:33:31.804760933 CET	53	63492	8.8.8.8	192.168.2.3
Jan 27, 2021 12:33:34.602005005 CET	60831	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:33:34.652759075 CET	53	60831	8.8.8.8	192.168.2.3
Jan 27, 2021 12:33:35.790699959 CET	60100	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:33:35.841535091 CET	53	60100	8.8.8.8	192.168.2.3
Jan 27, 2021 12:33:37.147110939 CET	53195	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:33:37.195096016 CET	53	53195	8.8.8.8	192.168.2.3
Jan 27, 2021 12:33:38.458867073 CET	50141	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:33:38.509751081 CET	53	50141	8.8.8.8	192.168.2.3
Jan 27, 2021 12:33:39.758410931 CET	53023	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:33:39.808118105 CET	53	53023	8.8.8.8	192.168.2.3
Jan 27, 2021 12:33:40.941373110 CET	49563	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:33:40.989288092 CET	53	49563	8.8.8.8	192.168.2.3
Jan 27, 2021 12:33:42.166100025 CET	51352	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:33:42.213928938 CET	53	51352	8.8.8.8	192.168.2.3
Jan 27, 2021 12:33:43.387100935 CET	59349	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:33:43.444571018 CET	53	59349	8.8.8.8	192.168.2.3
Jan 27, 2021 12:33:44.650142908 CET	57084	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:33:44.698065996 CET	53	57084	8.8.8.8	192.168.2.3
Jan 27, 2021 12:33:45.778295994 CET	58823	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:33:45.826289892 CET	53	58823	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 12:33:46.959475994 CET	57568	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:33:47.009632111 CET	53	57568	8.8.8.8	192.168.2.3
Jan 27, 2021 12:33:58.304991961 CET	50540	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:33:58.357912064 CET	53	50540	8.8.8.8	192.168.2.3
Jan 27, 2021 12:34:05.511758089 CET	54366	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:34:05.571175098 CET	53	54366	8.8.8.8	192.168.2.3
Jan 27, 2021 12:34:18.137455940 CET	53034	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:34:18.207076073 CET	53	53034	8.8.8.8	192.168.2.3
Jan 27, 2021 12:34:19.361601114 CET	57762	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:34:19.423527956 CET	53	57762	8.8.8.8	192.168.2.3
Jan 27, 2021 12:34:20.439914942 CET	55435	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:34:20.487991095 CET	53	55435	8.8.8.8	192.168.2.3
Jan 27, 2021 12:34:23.978684902 CET	50713	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:34:24.039310932 CET	53	50713	8.8.8.8	192.168.2.3
Jan 27, 2021 12:35:04.093718052 CET	56132	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:35:04.145981073 CET	53	56132	8.8.8.8	192.168.2.3
Jan 27, 2021 12:35:06.202208996 CET	58987	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:35:06.265650034 CET	53	58987	8.8.8.8	192.168.2.3
Jan 27, 2021 12:35:08.458524942 CET	56579	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:35:08.517349958 CET	53	56579	8.8.8.8	192.168.2.3
Jan 27, 2021 12:36:21.292306900 CET	60633	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:36:21.348989964 CET	53	60633	8.8.8.8	192.168.2.3
Jan 27, 2021 12:36:21.976433992 CET	61292	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:36:22.024369001 CET	53	61292	8.8.8.8	192.168.2.3
Jan 27, 2021 12:36:22.723779917 CET	63619	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:36:22.771917105 CET	53	63619	8.8.8.8	192.168.2.3
Jan 27, 2021 12:36:23.305397034 CET	64938	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:36:23.362088919 CET	53	64938	8.8.8.8	192.168.2.3
Jan 27, 2021 12:36:23.980076075 CET	61946	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:36:24.041855097 CET	53	61946	8.8.8.8	192.168.2.3
Jan 27, 2021 12:36:24.724802971 CET	64910	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:36:24.783817053 CET	53	64910	8.8.8.8	192.168.2.3
Jan 27, 2021 12:36:25.531107903 CET	52123	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:36:25.582056046 CET	53	52123	8.8.8.8	192.168.2.3
Jan 27, 2021 12:36:26.658972979 CET	56130	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:36:26.718672037 CET	53	56130	8.8.8.8	192.168.2.3
Jan 27, 2021 12:36:28.413674116 CET	56338	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:36:28.470185995 CET	53	56338	8.8.8.8	192.168.2.3
Jan 27, 2021 12:36:28.968753099 CET	59420	53	192.168.2.3	8.8.8.8
Jan 27, 2021 12:36:29.025866032 CET	53	59420	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 12:35:08.458524942 CET	192.168.2.3	8.8.8.8	0x5157	Standard query (0)	polar.argo ndns.net	A (IP address)	IN (0x0001)

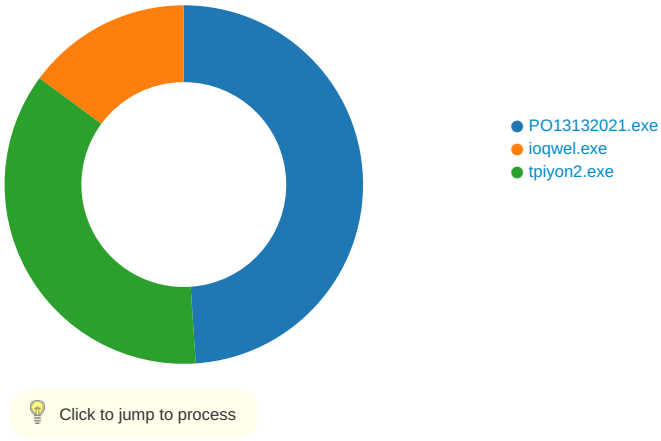
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 12:35:08.517349958 CET	8.8.8.8	192.168.2.3	0x5157	No error (0)	polar.argo ndns.net		91.210.107.22	A (IP address)	IN (0x0001)
Jan 27, 2021 12:35:08.517349958 CET	8.8.8.8	192.168.2.3	0x5157	No error (0)	polar.argo ndns.net		91.210.107.62	A (IP address)	IN (0x0001)
Jan 27, 2021 12:35:08.517349958 CET	8.8.8.8	192.168.2.3	0x5157	No error (0)	polar.argo ndns.net		91.210.107.53	A (IP address)	IN (0x0001)
Jan 27, 2021 12:35:08.517349958 CET	8.8.8.8	192.168.2.3	0x5157	No error (0)	polar.argo ndns.net		91.210.107.54	A (IP address)	IN (0x0001)
Jan 27, 2021 12:35:08.517349958 CET	8.8.8.8	192.168.2.3	0x5157	No error (0)	polar.argo ndns.net		91.210.107.52	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PO13132021.exe PID: 6960 Parent PID: 5792

General

Start time:	12:33:35
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\PO13132021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO13132021.exe'
Imagebase:	0x400000
File size:	725929 bytes
MD5 hash:	7C4C3A12F367DCD154ACCCE5948EBAEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nstBE1F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nstBE20.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
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	40589E	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Nla	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\Nla\ioqwel.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA
C:\Users\user\AppData\Local\Temp\Nla\zfngholtp.s	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA
C:\Users\user\AppData\Local\Temp\Nla\jsgwugqwc.ftb	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nstBE1F.tmp	success or wait	1	4036D8	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nstBE20.tmp	unknown	29668	8f 09 00 00 88 00 00 00 2c 01 00 00 03 00 00 00 ec 01 00 00 01 00 00 00 04 06 00 00 06 00 00 00 ac 06 00 00 00 00 00 00 ed 08 00 00 01 00 00 00 8f 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 a2 00 00 00 f1 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.......,......................	success or wait	71	405E82	WriteFile
C:\Users\user\AppData\Local\Temp\Nla\ioqwel.exe	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 16 73 44 90 52 12 2a c3 52 12 2a c3 52 12 2a c3 14 43 cb c3 50 12 2a c3 cc b2 ed c3 53 12 2a c3 5f 40 f5 c3 61 12 2a c3 5f 40 ca c3 e3 12 2a c3 5f 40 cb c3 67 12 2a c3 5b 6a a9 c3 5b 12 2a c3 5b 6a b9 c3 77 12 2a c3 52 12 2b c3 72 10 2a c3 e7 8c c0 c3 02 12 2a c3 e7 8c f5 c3 53 12 2a c3 5f 40 f1 c3 53 12 2a c3 52 12 bd c3 50 12 2a c3 e7 8c f4 c3 53 12 2a c3 52 69 63 68 52 12 2a	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........sD.R.*.R.*.R.*..C..P. *.....S.*._@..a.*._@....*._@ ..g.*.[j..[.*.[j..w.*.R.+.r.*... ....*.....S.*._@..S.*.R...P.*. ....S.*.RichR.*	success or wait	55	405E82	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Nla\zfngholtp.s	unknown	16384	47 6c 6f 62 61 6c 20 24 5a 33 32 33 32 64 64 79 38 69 35 69 20 3d 20 45 78 65 63 75 74 65 28 22 43 68 72 22 29 0d 0a 23 4e 6f 54 72 61 79 49 63 6f 6e 0d 0a 47 6c 6f 62 61 6c 20 24 52 33 30 38 6b 33 74 35 36 34 63 2c 20 24 54 33 31 70 38 65 2c 20 24 58 33 32 6f 32 74 6e 79 32 79 2c 20 24 41 33 33 33 79 37 74 65 6f 2c 20 24 49 33 34 69 69 69 2c 20 24 4e 33 35 33 66 76 36 0d 0a 46 6f 72 20 24 52 33 30 38 6b 33 74 35 36 34 63 20 3d 20 30 20 54 6f 20 52 61 6e 64 6f 6d 28 35 2c 20 38 2c 20 31 29 0d 0a 20 24 58 33 32 6f 32 74 6e 79 32 79 20 3d 20 30 0d 0a 20 46 6f 72 20 24 41 33 33 79 37 74 65 6f 20 3d 20 32 20 54 6f 20 31 30 30 0d 0a 20 20 24 54 33 31 70 38 65 20 3d 20 54 72 75 65 0d 0a 20 20 24 49 33 34 69 69 69 20 3d 20 32 0d 0a 20 20 57 68 69 6c 65 20 24 49 33	Global $Z3232ddy8i5i = Execute ("Chr")..#NoTrayIcon..Global $R308k3t564c, $T31p8e, $X32o2tny2y, $A33y7teo, $I34iii, $N353fv6..For $R308k3t564c = 0 To Random(5, 8, 1).. $X32o2tny2y = 0.. For $A33y7teo = 2 To 100.. $T31p8e = True.. $I34iii = 2.. While $I3	success or wait	24	405E82	WriteFile
C:\Users\user\AppData\Local\Temp\Nla\jsgwugqwc.ftb	unknown	16384	fa 5f d0 cf e2 9a 93 26 77 42 6e 75 d2 4b b7 5e 37 8e b4 4b f1 ed cb 84 15 43 67 40 18 78 86 0a 80 59 5b c2 53 82 99 7c 82 cc cc 94 57 09 f9 86 07 d1 bc a2 d4 04 73 5a d0 94 21 2d 70 c7 26 ea 82 c8 ed 8f 29 c0 0b 09 04 c0 26 0f a5 0f 6e ff 34 6c 83 17 8a 73 5c 84 83 90 86 62 7a 22 cb da a2 5d 5d a9 2f 96 46 a0 40 3a 36 4a ee 2b 04 c7 6f 7c ca 16 6c 44 2e ff b1 66 92 b2 74 6e d9 2f ae 97 71 9a 82 ca 2f fd 1e 30 0e 8b 3c 96 23 62 9a 75 0b 8d 44 18 06 be 93 f2 7e 69 d3 5f 8f 69 b8 6d b2 88 0e 25 4f 03 80 68 f4 a9 12 c6 c0 18 3a b0 5d 36 60 db 5f 30 88 ee 90 66 29 d0 ac 2f a4 12 3b b1 eb 13 88 90 f0 26 05 4b 2e 22 da 3b 82 75 ac ac 9d 4b da 13 d2 50 f0 c6 c1 12 3a 96 e9 f4 28 66 f8 d4 8a e6 05 2d 98 16 83 79 88 d2 37 4d 7f 33 a4 9d 9b 41 39 e9 8a 77 19 d1 00	._.....&wBnu.K.^7..K.....Cg @.x ...Y[.S..|....W.....sZ..!-p.&.....).....&...n.4l...s\... .bz"...]]./.F.@:6J.+..o|..lD.. .f..tn./..q.../..0..<.#b.u..D. ....~i._.i.m...%O..h......:.]6 `._0...f)../..;.....&.K.".;.u ...K...P....:...(f.....-...y.. 7M.3...A9..w...	success or wait	18	405E82	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PO13132021.exe	unknown	512	success or wait	70	405E53	ReadFile
C:\Users\user\Desktop\PO13132021.exe	unknown	16384	success or wait	43	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nstBE20.tmp	unknown	4	success or wait	1	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nstBE20.tmp	unknown	2447	success or wait	1	403280	ReadFile
C:\Users\user\AppData\Local\Temp\nstBE20.tmp	unknown	4	success or wait	3	405E53	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nstBE20.tmp	unknown	16384	success or wait	97	405E53	ReadFile

Analysis Process: ioqwel.exe PID: 6996 Parent PID: 6960

General

Start time:	12:33:36
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Local\Temp\Nla\ioqwel.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Nla\ioqwel.exe C:\Users\user\AppData\Local\Temp\Nla\zfngholtp.s
Imagebase:	0xab0000
File size:	893608 bytes
MD5 hash:	C56B5F0201A3B3DE53E561FE76912BFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.213456226.00000000032F0000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 5%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Nla\zfngholtp.s	unknown	65536	success or wait	7	AE12FD	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\zfngholtp.s	unknown	4096	end of file	2	AE12FD	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\zfngholtp.s	unknown	65536	success or wait	7	AE12FD	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\zfngholtp.s	unknown	4096	end of file	2	AE12FD	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\zfngholtp.s	unknown	65536	success or wait	1	AC427C	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\zfngholtp.s	unknown	65536	success or wait	5	AC39EF	ReadFile
C:\Users\user\AppData\Local\Temp\Nla\zfngholtp.s	unknown	65536	end of file	1	AC39EF	ReadFile

Analysis Process: tpiyon2.exe PID: 7028 Parent PID: 6996

General

Start time:	12:33:37
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Local\Temp\Nla\tpiyon2.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Nla\ioqwel.exe C:\Users\user\AppData\Local\Temp\Nla\zfngholtp.s
Imagebase:	0x400000
File size:	893608 bytes
MD5 hash:	535DD1329AEF11BF4654B3270F026D5B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.587931278.0000000003E01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.583608219.0000000000CA6000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.582750259.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.583897205.0000000002812000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000001.209476830.0000000000414000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.586869289.0000000002E01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.586869289.0000000002E01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.583855776.00000000027D0000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 21%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	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	72FB60AC	unknown
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	72FB60AC	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	72FB60AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	572143F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\947a1d13-4df2-49e4-8a2c-9fe3d081d395	unknown	4096	success or wait	1	572143F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	572143F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	572143F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	572143F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	572143F	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	572143F	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	572143F	ReadFile

Disassembly

Code Analysis