ID: 324081
Sample Name: PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe
Cookbook: default.jbs
Time: 10:30:16
Date: 28/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

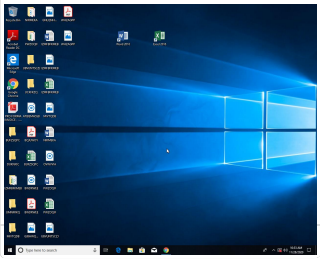
Analysis Report PRO FORMA INVOICE - - MAGAUTKCP ...

Overview

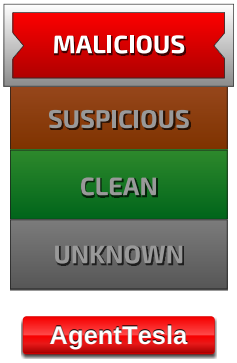
General Information

Sample Name:	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe
Analysis ID:	324081
MD5:	b3cb5b2bc5c303..
SHA1:	3fd8e55a12bdf35..
SHA256:	042ef647920e37e.
Tags:	exe

Most interesting Screenshot:



Detection

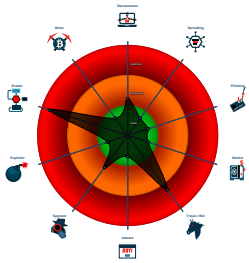


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Antivirus or Machine Learning detec…
- Contains functionality to check if a d…
- Contains functionality to check the p…

Classification



Startup

- **System is w10x64**
- PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe (PID: 6152 cmdline: 'C:\Users\user\Desktop\PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe' MD5: B3CB5B2BC5C3033B1008ED7F7F6312DB)
  - PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe (PID: 6944 cmdline: C:\Users\user\Desktop\PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe MD5: B3CB5B2BC5C3033B1008ED7F7F6312DB)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.918795043.00000000036E4000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.917038973.0000000002680000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.916512263.0000000002380000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000003.765764476.000000000086E000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.918550525.00000000027B7000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 4 entries

Unpacked PEs

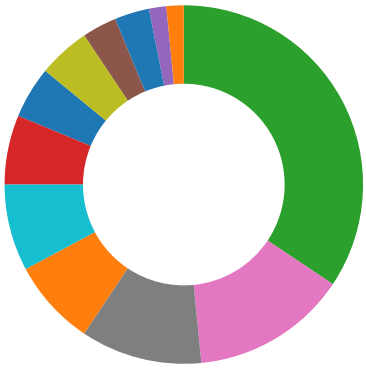
Source	Rule	Description	Author	Strings
11.2.PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe.2380000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
11.2.PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe.2680000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe.2380000.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe.2680000.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

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)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

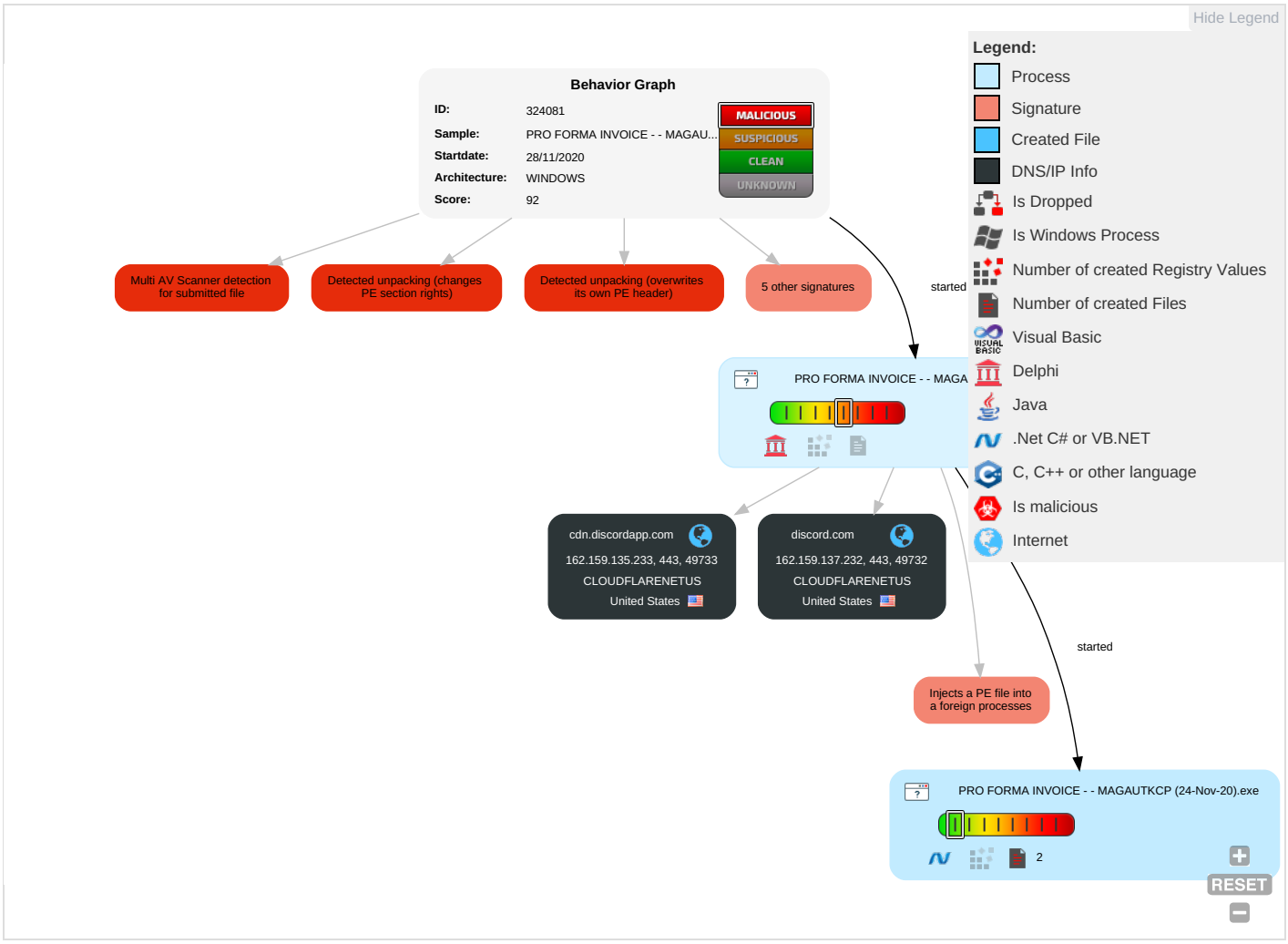
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co an
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	Process Injection 1 1 2	Virtualization/Sandbox Evasion 1 3	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	En Ch
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	No Ap La Pr
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Security Software Discovery 1 4 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ap La Pr
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Virtualization/Sandbox Evasion 1 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Pr Im
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Process Discovery 3	SSH	Keylogging	Data Transfer Size Limits	Fa Ch
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mi Co
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Account Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Us
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Ap La
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	W
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Information Discovery 1 2 4	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fil Pr

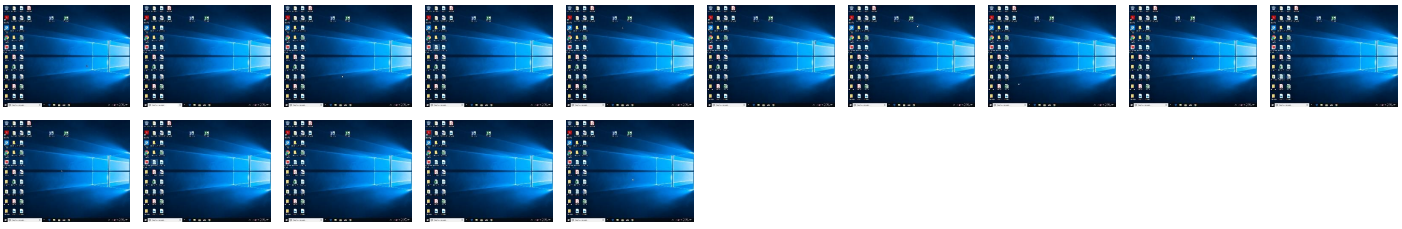
Behavior Graph



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
PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe	56%	ReversingLabs	Win32.Infostealer.Fareit	
PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.1.PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ftp://ftp.kunwersachdev.com/maerst	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://JvKUzM.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://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

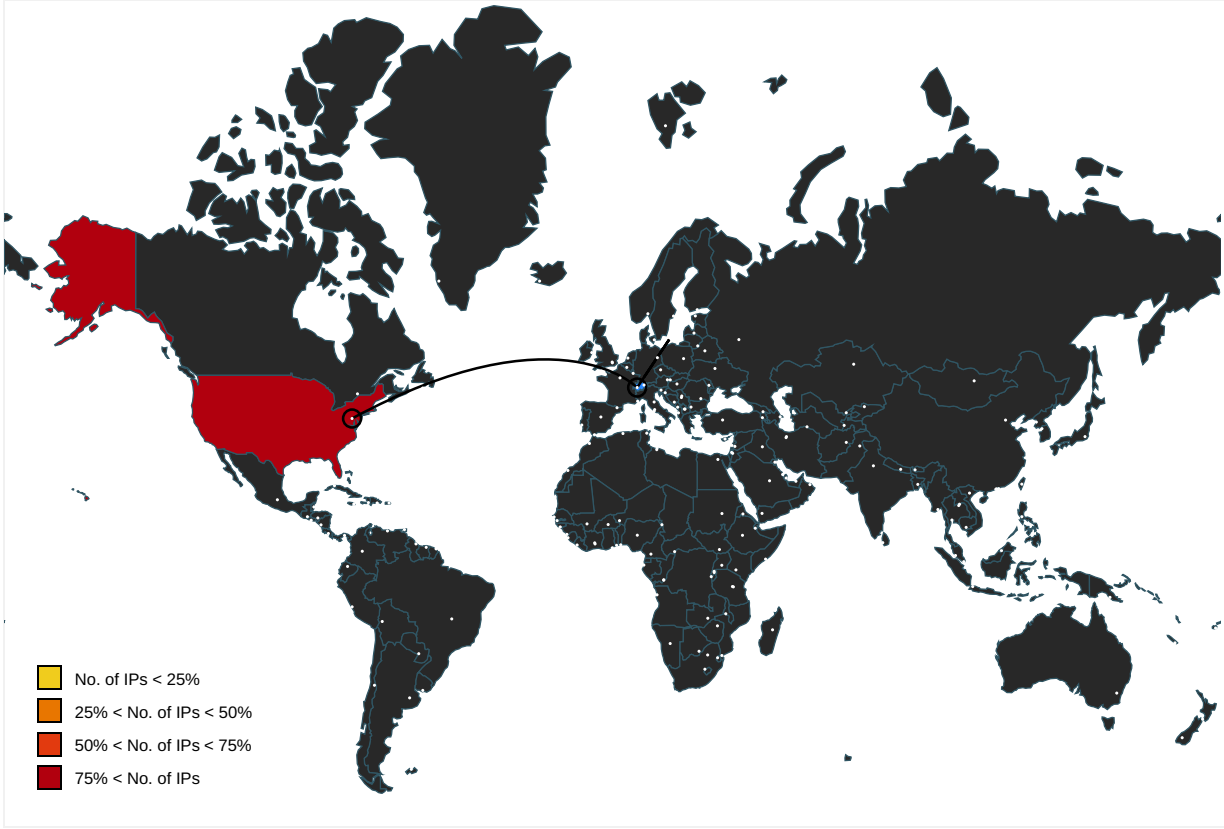
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
discord.com	162.159.137.232	true	false		unknown
cdn.discordapp.com	162.159.135.233	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ftp://ftp.kunwersachdev.com/maerst	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe, 0000000B.000000002.918550525.00000000027B7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe, 0000000B.000000002.918550525.00000000027B7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe, 0000000B.000000002.918550525.00000000027B7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://JvKUzM.com	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe, 0000000B.000000002.918550525.00000000027B7000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://gorohov.narod.ru/index.htmS	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe	false		high
http://gorohov.narod.ru/index.htm	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe, 0000000B.000000002.918550525.00000000027B7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe, 0000000B.000000002.918550525.00000000027B7000.00000004.00000001.sdmp	false		high
http://https://api.ipify.orgGETMozilla/5.0	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe, 0000000B.000000002.918550525.00000000027B7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.159.137.232	unknown	United States		13335	CLOUDFLARENETUS	false
162.159.135.233	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324081
Start date:	28.11.2020
Start time:	10:30:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).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:	19
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:	mal92.troj.evad.winEXE@3/0@2/2

EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.8% (good quality ratio 4.6%) • Quality average: 82.9% • Quality standard deviation: 26.9%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 51.11.168.160, 92.122.213.194, 92.122.213.247, 52.255.188.83, 2.20.142.209, 2.20.142.210, 52.155.217.156, 20.54.26.129, 51.104.144.132 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/324081/sample/PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe

Simulations

Behavior and APIs

Time	Type	Description
10:31:06	API Interceptor	406x Sleep call for process: PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.159.137.232	MT103---USD42880.45---20201127--dbs--9900.exe	Get hash	malicious	Browse	
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	
	Scan 25112020 pdf.exe	Get hash	malicious	Browse	
	Q21rQw2C4o.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	tzjEwwwbqK.exe	Get hash	malicious	Browse	
	oUI0jQS8xQ.exe	Get hash	malicious	Browse	
	NyUnwsFSCa.exe	Get hash	malicious	Browse	
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	
	LAX28102020HBL_AMSLAX1056_CTLQD06J0BL_PO_DTH266278_RFQ.exe	Get hash	malicious	Browse	
	8fJPaTfN8D.exe	Get hash	malicious	Browse	
	LJLMG5Syza.exe	Get hash	malicious	Browse	
	oAkfKRTCvN.exe	Get hash	malicious	Browse	
	eybgvwBamW.exe	Get hash	malicious	Browse	
	R#U00d6SLER Puchase_tcs 10-28-2020,pdf.exe	Get hash	malicious	Browse	
	#U8ba2#U5355#U786e#U8ba4,pdf.exe	Get hash	malicious	Browse	
	Documentos_ordine.exe	Get hash	malicious	Browse	
	ShipmentReceipt.exe	Get hash	malicious	Browse	
	ShipmentReceipt.exe	Get hash	malicious	Browse	
	PO102620.exe	Get hash	malicious	Browse	
	Albawardi Group Project offer description 67846746 3756382020.exe	Get hash	malicious	Browse	
162.159.135.233	Vessel details.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/780175015496777751/781048233136226304/mocux.exe
	Teklif Rusya 24 09 2020.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/733818080668680222/758418625429372978/p2.jpg

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
discord.com	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.128.233
	XcOxlmOz4D.exe	Get hash	malicious	Browse	• 162.159.136.232
	fAhW3JEGaZ.exe	Get hash	malicious	Browse	• 162.159.136.232
	HIp08HPg20.exe	Get hash	malicious	Browse	• 162.159.128.233
	MT103---USD42880.45---20201127--dbs--9900.exe	Get hash	malicious	Browse	• 162.159.137.232
	caw.exe	Get hash	malicious	Browse	• 162.159.138.232
	lxpo.exe	Get hash	malicious	Browse	• 162.159.128.233
	SpecificationX20202611.xlsx	Get hash	malicious	Browse	• 162.159.136.232
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 162.159.137.232
	Scan 25112020 pdf.exe	Get hash	malicious	Browse	• 162.159.137.232
	Piraeus Bank_swift_.exe	Get hash	malicious	Browse	• 162.159.128.233
	Q21rQw2C4o.exe	Get hash	malicious	Browse	• 162.159.137.232
	Q21rQw2C4o.exe	Get hash	malicious	Browse	• 162.159.128.233
	tzjEwwwbqK.exe	Get hash	malicious	Browse	• 162.159.136.232
	DHL_Express_Consignment_Details.exe	Get hash	malicious	Browse	• 162.159.138.232
	New Microsoft Office Excel Worksheet.xlsx	Get hash	malicious	Browse	• 162.159.136.232
	Komfkim_Signed_.exe	Get hash	malicious	Browse	• 162.159.135.232

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	oUI0jQS8xQ.exe	Get hash	malicious	Browse	• 162.159.137.232
	USD67,884.08_Payment_Advise_9083008849.exe	Get hash	malicious	Browse	• 162.159.136.232
	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	Get hash	malicious	Browse	• 162.159.138.232
cdn.discordapp.com	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.129.233
	OVERDUE INVOICE.xls	Get hash	malicious	Browse	• 162.159.129.233
	MT103---USD42880.45---20201127--dbs--9900.exe	Get hash	malicious	Browse	• 162.159.129.233
	Vessel details.doc	Get hash	malicious	Browse	• 162.159.135.233
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 162.159.130.233
	Scan 25112020 pdf.exe	Get hash	malicious	Browse	• 162.159.135.233
	Piraeus Bank_swift_.exe	Get hash	malicious	Browse	• 162.159.129.233
	Q21rQw2C4o.exe	Get hash	malicious	Browse	• 162.159.130.233
	Q21rQw2C4o.exe	Get hash	malicious	Browse	• 162.159.133.233
	tzjEwwwbqK.exe	Get hash	malicious	Browse	• 162.159.130.233
	DHL_Express_Consignment_Details.exe	Get hash	malicious	Browse	• 162.159.133.233
	New Microsoft Office Excel Worksheet.xlsx	Get hash	malicious	Browse	• 162.159.129.233
	INV SF2910202.doc	Get hash	malicious	Browse	• 162.159.135.233
	Komfkim_Signed_.exe	Get hash	malicious	Browse	• 162.159.129.233
	oUI0jQS8xQ.exe	Get hash	malicious	Browse	• 162.159.130.233
	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	Get hash	malicious	Browse	• 162.159.135.233
	NyUnwsFSCa.exe	Get hash	malicious	Browse	• 162.159.133.233
	1099008FEDEX_090887766.xls	Get hash	malicious	Browse	• 162.159.129.233
	1099008FEDEX_090887766.xls	Get hash	malicious	Browse	• 162.159.134.233
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	• 162.159.135.233

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.135.233
	XcOxlmOz4D.exe	Get hash	malicious	Browse	• 162.159.136.232
	fAhW3JEGaZ.exe	Get hash	malicious	Browse	• 162.159.136.232
	HIp08HPg20.exe	Get hash	malicious	Browse	• 104.23.98.190
	case.8920.xls	Get hash	malicious	Browse	• 104.27.186.55
	case.8920.xls	Get hash	malicious	Browse	• 172.67.212.16
	OVERDUE INVOICE.xls	Get hash	malicious	Browse	• 172.67.143.180
	Venom.exe	Get hash	malicious	Browse	• 104.23.98.190
	PO348578.jar	Get hash	malicious	Browse	• 104.23.99.190
	MT103---USD42880.45---20201127--dbs--9900.exe	Get hash	malicious	Browse	• 162.159.129.233
	notif8372.xls	Get hash	malicious	Browse	• 104.24.117.11
	notif8372.xls	Get hash	malicious	Browse	• 172.67.222.45
	SecuriteInfo.com.Heur.23770.xls	Get hash	malicious	Browse	• 104.31.87.226
	2020-11-27-ZLoader-DLL-example-01.dll	Get hash	malicious	Browse	• 172.67.155.205
	2020-11-27-ZLoader-DLL-example-02.dll	Get hash	malicious	Browse	• 172.67.155.205
	2020-11-27-ZLoader-DLL-example-03.dll	Get hash	malicious	Browse	• 104.27.143.240
	SecuriteInfo.com.Heur.23770.xls	Get hash	malicious	Browse	• 104.31.86.226

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Final_report_2020.html	Get hash	malicious	Browse	• 104.16.18.94
	norit.dll	Get hash	malicious	Browse	• 104.31.69.174
	380000_USD_INV_011740_NOV_2020.jar	Get hash	malicious	Browse	• 104.20.22.46
CLOUDFLARENETUS	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.135.233
	XcOxlmOz4D.exe	Get hash	malicious	Browse	• 162.159.136.232
	fAhW3JEGaZ.exe	Get hash	malicious	Browse	• 162.159.136.232
	HIp08HPg20.exe	Get hash	malicious	Browse	• 104.23.98.190
	case.8920.xls	Get hash	malicious	Browse	• 104.27.186.55
	case.8920.xls	Get hash	malicious	Browse	• 172.67.212.16
	OVERDUE INVOICE.xls	Get hash	malicious	Browse	• 172.67.143.180
	Venom.exe	Get hash	malicious	Browse	• 104.23.98.190
	PO348578.jar	Get hash	malicious	Browse	• 104.23.99.190
	MT103---USD42880.45---20201127--dbs--9900.exe	Get hash	malicious	Browse	• 162.159.129.233
	notif8372.xls	Get hash	malicious	Browse	• 104.24.117.11
	notif8372.xls	Get hash	malicious	Browse	• 172.67.222.45
	SecuriteInfo.com.Heur.23770.xls	Get hash	malicious	Browse	• 104.31.87.226
	2020-11-27-ZLoader-DLL-example-01.dll	Get hash	malicious	Browse	• 172.67.155.205
	2020-11-27-ZLoader-DLL-example-02.dll	Get hash	malicious	Browse	• 172.67.155.205
	2020-11-27-ZLoader-DLL-example-03.dll	Get hash	malicious	Browse	• 104.27.143.240
	SecuriteInfo.com.Heur.23770.xls	Get hash	malicious	Browse	• 104.31.86.226
	Final_report_2020.html	Get hash	malicious	Browse	• 104.16.18.94
	norit.dll	Get hash	malicious	Browse	• 104.31.69.174
	380000_USD_INV_011740_NOV_2020.jar	Get hash	malicious	Browse	• 104.20.22.46

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.135.233
	caw.exe	Get hash	malicious	Browse	• 162.159.135.233
	6znqz0d1.dll	Get hash	malicious	Browse	• 162.159.135.233
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 162.159.135.233
	INV-FATURA010009.xlsx	Get hash	malicious	Browse	• 162.159.135.233
	2zv940v7.dll	Get hash	malicious	Browse	• 162.159.135.233
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 162.159.135.233
	Izezma64.dll	Get hash	malicious	Browse	• 162.159.135.233
	fuxenm32.dll	Get hash	malicious	Browse	• 162.159.135.233
	api-cdef.dll	Get hash	malicious	Browse	• 162.159.135.233
	Scan 25112020 pdf.exe	Get hash	malicious	Browse	• 162.159.135.233
	tarifvertrag_igbce_weihnachtsgeld_k#U00fcndigung.js	Get hash	malicious	Browse	• 162.159.135.233
	tarifvertrag_igbce_weihnachtsgeld_k#U00fcndigung.js	Get hash	malicious	Browse	• 162.159.135.233
	Piraeus Bank_swift_.exe	Get hash	malicious	Browse	• 162.159.135.233
	FxzOwcXb7x.exe	Get hash	malicious	Browse	• 162.159.135.233
	Izipubob.dll	Get hash	malicious	Browse	• 162.159.135.233
	nivude1.dll	Get hash	malicious	Browse	• 162.159.135.233
	Accesshover.dll	Get hash	malicious	Browse	• 162.159.135.233
	data7195700.xls	Get hash	malicious	Browse	• 162.159.135.233
	PAYMENT COPY.xls	Get hash	malicious	Browse	• 162.159.135.233

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.110241254206797
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:	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe
File size:	1218752
MD5:	b3cb5b2bc5c3033b1008ed7f7f6312db
SHA1:	3fd8e55a12bdf35200ee43e210951825ad0293d3
SHA256:	042ef647920e37e8da471c1bfbc36490ee6bf93ceee75cd90161823ae74d458b
SHA512:	3724f52089d06f1260f1b6c0ddf73326d44e5b16a12fc99b868c831e481b1edab29fac4695f64e222679d936789455f6c2ce38e5cdfc595d73352faafd321836
SSDEEP:	24576:3RVtvQ+csIDccuZGhe1ppCmfwybRm8zQKtALblKCeNRbO+v:3R/ovVcOM1pJwYFzQ0t
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	b2989692969ed26a

Static PE Info

General

Entrypoint:	0x47f698
Entrypoint Section:	CODE
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, UP_SYSTEM_ONLY, LARGE_ADDRESS_AWARE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI, RELOCS_STRIPPED
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:	191f8035b5c11d5de8fd20cfdada0df2

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Microsoft Code Signing PCA, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 8/18/2016 10:17:17 PM 11/2/2017 9:17:17 PM
Subject Chain	• CN=Microsoft Corporation, OU=MOPR, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Version:	3
Thumbprint MD5:	3B66EDDAB891B79FEDB150AC2C59DB3A
Thumbprint SHA-1:	98ED99A67886D020C564923B7DF25E9AC019DF26
Thumbprint SHA-256:	57DD481BF26C0A55C3E867B2D6C6978BEAF5CE3509325CA2607D853F9349A9FF
Serial:	330000014096A9EE7056FECC07000100000140

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 0047F418h
call 00007F07A4909C35h
push 0000001Eh
pop ebx
push eax
mov eax, dword ptr [00481FE8h]
mov eax, dword ptr [eax]
call 00007F07A4960A39h
mov eax, dword ptr [00481FE8h]
mov eax, dword ptr [eax]
mov edx, 0047F708h
call 00007F07A4960628h
mov ecx, dword ptr [00481F6Ch]
mov eax, dword ptr [00481FE8h]
mov eax, dword ptr [eax]
mov edx, dword ptr [0047EF20h]
call 00007F07A4960A28h
mov eax, dword ptr [00481FE8h]
mov eax, dword ptr [eax]
mov byte ptr [eax+5Bh], 00000000h
mov eax, dword ptr [00481FE8h]
mov eax, dword ptr [eax]
call 00007F07A4960A91h
call 00007F07A4907724h
add byte ptr [eax], al
add bh, bh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x85000	0x24ca	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x93000	0x97c00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x124400	0x54c0	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8a000	0x8f34	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x89000	0x18	.rdata

Name	Virtual Address	Virtual Size	Is in Section
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	0x7e714	0x7e800	False	0.523837002841	data	6.52444996172	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x80000	0x219c	0x2200	False	0.390969669118	data	4.54957969266	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x83000	0x1135	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x85000	0x24ca	0x2600	False	0.354851973684	data	4.81311536495	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x88000	0x40	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x89000	0x18	0x200	False	0.05078125	data	0.184150656087	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x8a000	0x8f34	0x9000	False	0.559760199653	data	6.63092268857	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x93000	0x97c00	0x97c00	False	0.509374678233	data	6.97981181424	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x93c0c	0x134	data		
RT_CURSOR	0x93d40	0x134	data		
RT_CURSOR	0x93e74	0x134	data		
RT_CURSOR	0x93fa8	0x134	data		
RT_CURSOR	0x940dc	0x134	data		
RT_CURSOR	0x94210	0x134	data		
RT_CURSOR	0x94344	0x134	data		
RT_BITMAP	0x94478	0x1d0	data		
RT_BITMAP	0x94648	0x1e4	data		
RT_BITMAP	0x9482c	0x1d0	data		
RT_BITMAP	0x949fc	0x1d0	data		
RT_BITMAP	0x94bcc	0x1d0	data		
RT_BITMAP	0x94d9c	0x1d0	data		
RT_BITMAP	0x94f6c	0x1d0	data		
RT_BITMAP	0x9513c	0x1d0	data		
RT_BITMAP	0x9530c	0x1d0	data		
RT_BITMAP	0x954dc	0x1d0	data		
RT_BITMAP	0x956ac	0xe8	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x95794	0x10a8	data	English	United States
RT_ICON	0x9683c	0x25a8	data	English	United States
RT_ICON	0x98de4	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 240, next used block 251658240	English	United States
RT_ICON	0x9d00c	0x5488	data	English	United States
RT_ICON	0xa2494	0xac5c	data	English	United States
RT_DIALOG	0xad0f0	0x52	data		
RT_STRING	0xad144	0x314	data		
RT_STRING	0xad458	0x1dc	data		
RT_STRING	0xad634	0x154	data		
RT_STRING	0xad788	0x3a4	data		
RT_STRING	0xadb2c	0x4bc	data		
RT_STRING	0xadfe8	0xc0	data		
RT_STRING	0xae0a8	0xfc	data		

Name	RVA	Size	Type	Language	Country
RT_STRING	0xae1a4	0x120	data		
RT_STRING	0xae2c4	0x4c0	data		
RT_STRING	0xae784	0x350	data		
RT_STRING	0xaead4	0x39c	data		
RT_STRING	0xaee70	0x3b0	data		
RT_STRING	0xaf220	0xf0	data		
RT_STRING	0xaf310	0xc0	data		
RT_STRING	0xaf3d0	0x2d8	data		
RT_STRING	0xaf6a8	0x494	data		
RT_STRING	0xafb3c	0x3ac	data		
RT_STRING	0xafee8	0x2d4	data		
RT_RCDATA	0xb01bc	0x10	data		
RT_RCDATA	0xb01cc	0x350	data		
RT_RCDATA	0xb051c	0x7859a	GIF image data, version 89a, 577 x 188	English	United States
RT_RCDATA	0x128ab8	0x1f39	Delphi compiled form 'T__882643936'		
RT_GROUP_CURSOR	0x12a9f4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x12aa08	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x12aa1c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x12aa30	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x12aa44	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x12aa58	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x12aa6c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0x12aa80	0x4c	data	English	United States

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetTickCount, QueryPerformanceCounter, GetVersion, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, WriteFile, UnhandledExceptionFilter, RtlUnwind, RaiseException, GetStdHandle
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, lstrcmpiA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtect, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MultiByteToWideChar, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, GetACP, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FindResourceA, FindFirstFileA, FindClose, FileTimeToLocalFileTime, FileTimeToDosDateTime, EnumCalendarInfoA, EnterCriticalSection, DeleteFileA, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
gdi32.dll	UnrealizeObject, StretchBlt, SetWindowOrgEx, SetWinMetaFileBits, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SaveDC, RestoreDC, Rectangle, RectVisible, RealizePalette, Polyline, Polygon, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPointA, GetTextExtentPoint32A, GetTextAlign, GetSystemPaletteEntries, GetStockObject, GetROP2, GetPolyFillMode, GetPixelFormat, GetPixel, GetPaletteEntries, GetObjectA, GetMapMode, GetGraphicsMode, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetDCPenColor, GetDCBrushColor, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBkMode, GetBkColor, GetBitmapBits, GdiFlush, ExcludeClipRect, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt

DLL	Import
user32.dll	CreateWindowExA, WindowFromPoint, WinHelpA, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, ShowCaret, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClipboardData, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, 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, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, HideCaret, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, EmptyClipboard, DrawTextA, DrawStateA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, CloseClipboard, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerBuffA, CharLowerA, CharUpperBuffA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayGetElement, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopyInd, VariantCopy, VariantClear, VariantInit
ole32.dll	CoUninitialize, CoInitialize
oleaut32.dll	GetErrorInfo, SysFreeString
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_SetImageCount, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create
shell32.dll	ShellExecuteA
winmm.dll	sndPlaySoundA

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 68

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 10:31:07.618732929 CET	49732	443	192.168.2.4	162.159.137.232
Nov 28, 2020 10:31:07.635231018 CET	443	49732	162.159.137.232	192.168.2.4
Nov 28, 2020 10:31:07.635396004 CET	49732	443	192.168.2.4	162.159.137.232
Nov 28, 2020 10:31:07.636028051 CET	49732	443	192.168.2.4	162.159.137.232
Nov 28, 2020 10:31:07.652529955 CET	443	49732	162.159.137.232	192.168.2.4
Nov 28, 2020 10:31:07.652559996 CET	443	49732	162.159.137.232	192.168.2.4
Nov 28, 2020 10:31:07.652657032 CET	49732	443	192.168.2.4	162.159.137.232
Nov 28, 2020 10:31:07.731426954 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:07.747754097 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:07.747883081 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:07.797060966 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:07.813452005 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:07.815418959 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:07.815448046 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:07.815462112 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:07.815733910 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:07.865027905 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:07.881252050 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:07.897581100 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:07.898933887 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:07.945055008 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.013133049 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.029519081 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057188988 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057210922 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057224035 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057240963 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057255030 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057267904 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057281017 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057291031 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057296991 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057316065 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057327986 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057341099 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057343960 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057358027 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057373047 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057403088 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057410002 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057410002 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057429075 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057446957 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057462931 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057463884 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057482004 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057499886 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057512999 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057518005 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057522058 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057531118 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057547092 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057565928 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057583094 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057595968 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057600975 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057609081 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057614088 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057631016 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057646036 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057662964 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057677984 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057678938 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057683945 CET	49733	443	192.168.2.4	162.159.135.233

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 10:31:08.057698011 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057714939 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057729006 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057733059 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057734013 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057750940 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057765961 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057769060 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057784081 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057800055 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057815075 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057816982 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057835102 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057852983 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057856083 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057871103 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057887077 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057899952 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057900906 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057904005 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057917118 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057934999 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057939053 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057951927 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057971001 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.057986021 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.057991028 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.058003902 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.058007956 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.058027029 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.058043957 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.058054924 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.058062077 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.058079004 CET	443	49733	162.159.135.233	192.168.2.4
Nov 28, 2020 10:31:08.058094025 CET	49733	443	192.168.2.4	162.159.135.233
Nov 28, 2020 10:31:08.058094978 CET	443	49733	162.159.135.233	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 10:31:02.219085932 CET	55854	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:02.246105909 CET	53	55854	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:07.560221910 CET	64549	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:07.587306976 CET	53	64549	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:07.702680111 CET	63153	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:07.729708910 CET	53	63153	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:28.383827925 CET	52991	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:28.411088943 CET	53	52991	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:34.247920990 CET	53700	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:35.273853064 CET	53700	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:36.078322887 CET	51726	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:36.241617918 CET	53	51726	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:36.241916895 CET	53	53700	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:36.242775917 CET	53	53700	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:36.987870932 CET	56794	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:37.014924049 CET	53	56794	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:37.733671904 CET	56534	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:37.769320965 CET	53	56534	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:38.429485083 CET	56627	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:38.456552982 CET	53	56627	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:39.143574953 CET	56621	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:39.170844078 CET	53	56621	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:39.872354984 CET	63116	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:39.910217047 CET	53	63116	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 10:31:40.799295902 CET	64078	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:40.826457024 CET	53	64078	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:49.510163069 CET	64801	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:49.546915054 CET	53	64801	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:54.236198902 CET	61721	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:54.279809952 CET	53	61721	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:54.814912081 CET	51255	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:54.868314981 CET	53	51255	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:55.420306921 CET	61522	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:55.455759048 CET	53	61522	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:55.775741100 CET	52337	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:55.811485052 CET	53	52337	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:56.188901901 CET	55046	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:56.224395037 CET	53	55046	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:56.684010983 CET	49612	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:56.719657898 CET	53	49612	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:57.369980097 CET	49285	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:57.407788992 CET	53	49285	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:58.073167086 CET	50601	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:58.108619928 CET	53	50601	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:59.318715096 CET	60875	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:59.354480982 CET	53	60875	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:59.681447029 CET	56448	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:59.717175961 CET	53	56448	8.8.8.8	192.168.2.4
Nov 28, 2020 10:31:59.858293056 CET	59172	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:31:59.909159899 CET	53	59172	8.8.8.8	192.168.2.4
Nov 28, 2020 10:32:05.831170082 CET	62420	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:32:05.868024111 CET	53	62420	8.8.8.8	192.168.2.4
Nov 28, 2020 10:32:12.090886116 CET	60579	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:32:12.117989063 CET	53	60579	8.8.8.8	192.168.2.4
Nov 28, 2020 10:32:12.799681902 CET	50183	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:32:12.826797962 CET	53	50183	8.8.8.8	192.168.2.4
Nov 28, 2020 10:32:14.314152956 CET	61531	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:32:14.341248989 CET	53	61531	8.8.8.8	192.168.2.4
Nov 28, 2020 10:32:15.578613043 CET	49228	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:32:15.605720043 CET	53	49228	8.8.8.8	192.168.2.4
Nov 28, 2020 10:32:17.442347050 CET	59794	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:32:17.477639914 CET	53	59794	8.8.8.8	192.168.2.4
Nov 28, 2020 10:32:44.223612070 CET	55916	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:32:44.250850916 CET	53	55916	8.8.8.8	192.168.2.4
Nov 28, 2020 10:32:45.968452930 CET	52752	53	192.168.2.4	8.8.8.8
Nov 28, 2020 10:32:46.004127026 CET	53	52752	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 28, 2020 10:31:07.560221910 CET	192.168.2.4	8.8.8.8	0x6e3c	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Nov 28, 2020 10:31:07.702680111 CET	192.168.2.4	8.8.8.8	0x3a8	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 28, 2020 10:31:07.587306976 CET	8.8.8.8	192.168.2.4	0x6e3c	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:31:07.587306976 CET	8.8.8.8	192.168.2.4	0x6e3c	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:31:07.587306976 CET	8.8.8.8	192.168.2.4	0x6e3c	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:31:07.587306976 CET	8.8.8.8	192.168.2.4	0x6e3c	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 28, 2020 10:31:07.587306976 CET	8.8.8.8	192.168.2.4	0x6e3c	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Nov 28, 2020 10:31:07.729708910 CET	8.8.8.8	192.168.2.4	0x3a8	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:31:07.729708910 CET	8.8.8.8	192.168.2.4	0x3a8	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:31:07.729708910 CET	8.8.8.8	192.168.2.4	0x3a8	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:31:07.729708910 CET	8.8.8.8	192.168.2.4	0x3a8	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Nov 28, 2020 10:31:07.729708910 CET	8.8.8.8	192.168.2.4	0x3a8	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)

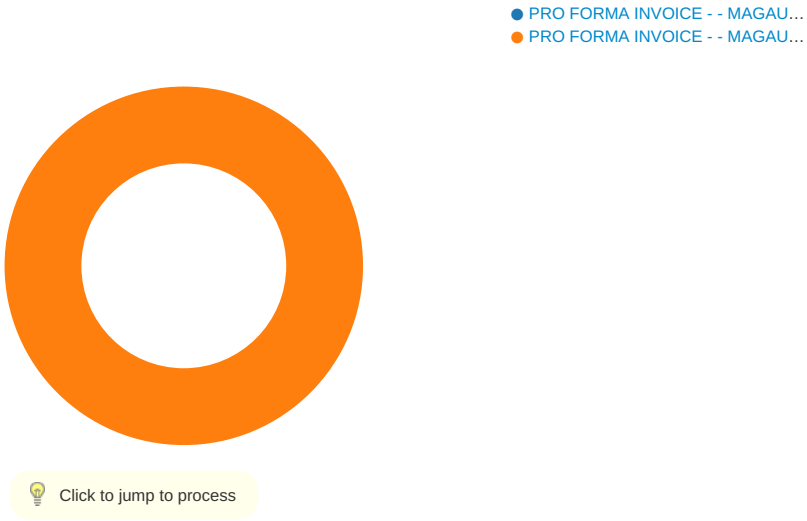
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 28, 2020 10:31:07.815462112 CET	162.159.135.233	443	192.168.2.4	49733	CN=ssl711320.cloudflaressl.com CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 27 01:00:00 CET 2020 Thu Sep 25 02:00:00 CEST 2014 Thu Jan 01 01:00:00 CET 2004	Thu May 06 01:59:59 CEST 2021 Tue Sep 25 01:59:59 CEST 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		
					CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe PID: 6152
Parent PID: 5940

General

Start time:	10:31:05
Start date:	28/11/2020
Path:	C:\Users\user\Desktop\PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe'
Imagebase:	0x400000
File size:	1218752 bytes
MD5 hash:	B3CB5B2BC5C3033B1008ED7F7F6312DB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe PID: 6944
Parent PID: 6152

General

Start time:	10:31:59
Start date:	28/11/2020
Path:	C:\Users\user\Desktop\PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe
Imagebase:	0x400000
File size:	1218752 bytes
MD5 hash:	B3CB5B2BC5C3033B1008ED7F7F6312DB
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: 0000000B.00000002.918795043.00000000036E4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.917038973.0000000002680000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.916512263.0000000002380000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000003.765764476.000000000086E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.918550525.00000000027B7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.918550525.00000000027B7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.916402342.00000000022A6000.00000004.00000001.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	6D3BCF06	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	6D3BCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D395705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D39CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C301B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C301B4F	ReadFile

Disassembly

Code Analysis