ID: 323965
Sample Name: MT103---USD42880.45---20201127--dbs--9900.exe
Cookbook: default.jbs
Time: 00:04:55
Date: 28/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

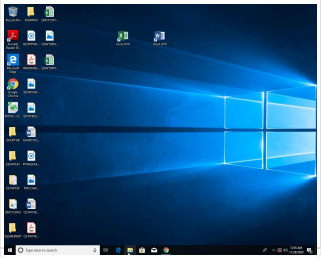
Analysis Report MT103---USD42880.45---20201127--dbs-…

Overview

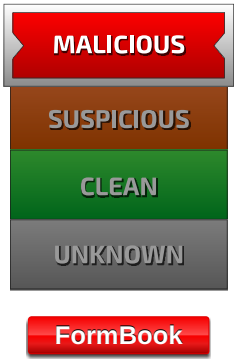
General Information

Sample Name:	MT103---USD42880.45---20201127--dbs--9900.exe
Analysis ID:	323965
MD5:	d7545487bde794..
SHA1:	f4728d4c214b028.
SHA256:	4d39dfd975de3e9.
Tags:	exe

Most interesting Screenshot:



Detection

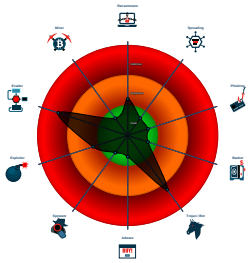


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Tries to detect virtualization through…
- Antivirus or Machine Learning detec…
- Checks if the current process is bein…
- Contains functionality for execution …
- Contains functionality to access load…
- Contains functionality to call native f…

Classification



Startup

- **System is w10x64**
- MT103---USD42880.45---20201127--dbs--9900.exe (PID: 5504 cmdline: 'C:\Users\user\Desktop\MT103---USD42880.45---20201127--dbs--9900.exe' MD5: D7545487BDE794DE42B3A655F3664C8D)
  - MT103---USD42880.45---20201127--dbs--9900.exe (PID: 2416 cmdline: C:\Users\user\Desktop\MT103---USD42880.45---20201127--dbs--9900.exe MD5: D7545487BDE794DE42B3A655F3664C8D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.214074450.0000000004C67000.00000020.00000001.sdmp	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0xde8:$file: URL= • 0xdcc:$url_explicit: [InternetShortcut]
00000000.00000002.214074450.0000000004C67000.00000020.00000001.sdmp	Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0xe14:$icon: IconFile= • 0xdcc:$url_explicit: [InternetShortcut]
00000000.00000002.214175689.0000000004CC0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.214175689.0000000004CC0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.214175689.0000000004CC0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
Click to see the 9 entries				

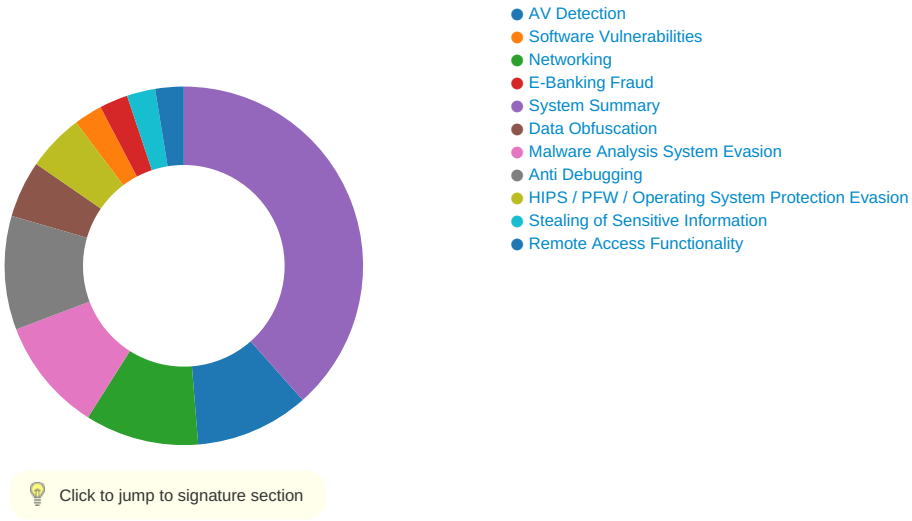
Unpacked PEs

Source	Rule	Description	Author	Strings
1.1.MT103---USD42880.45---20201127--dbs--9900.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.MT103---USD42880.45---20201127--dbs--9900.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.1.MT103---USD42880.45---20201127--dbs--9900.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
0.2.MT103---USD42880.45---20201127--dbs--9900.exe.4cc0000.9.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.MT103---USD42880.45---20201127--dbs--9900.exe.4cc0000.9.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected FormBook

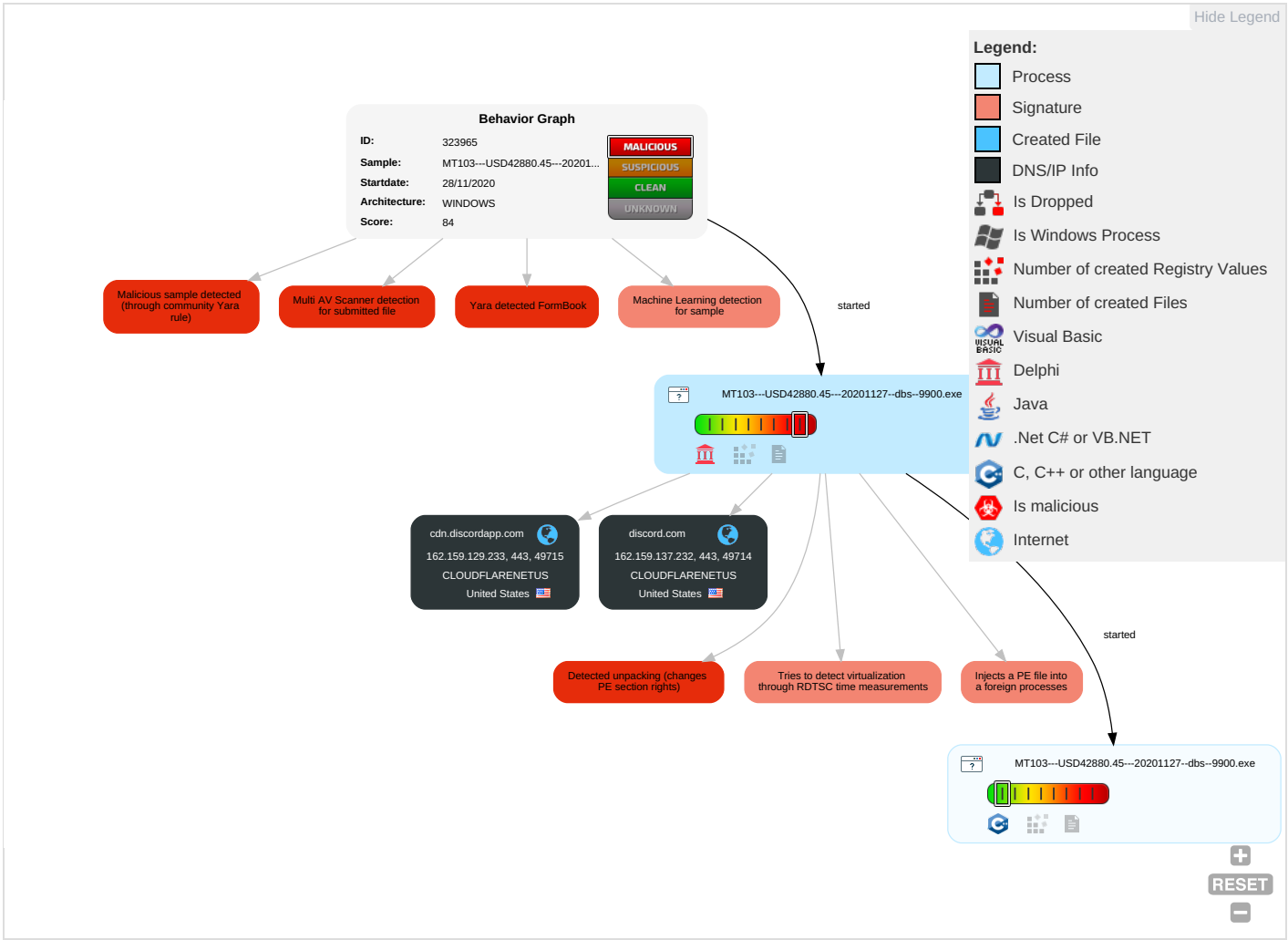
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1 1	Virtualization/Sandbox Evasion 2	OS Credential Dumping	Security Software Discovery 1 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 1 1	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 1	LSA Secrets	System Information Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati

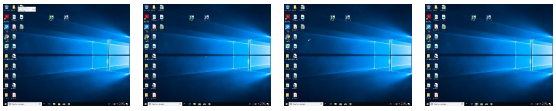
Behavior Graph



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
MT103---USD42880.45---20201127--dbs--9900.exe	37%	Virustotal		Browse
MT103---USD42880.45---20201127--dbs--9900.exe	48%	ReversingLabs	Win32.Trojan.Strictor	
MT103---USD42880.45---20201127--dbs--9900.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.MT103---USD42880.45---20201127--dbs--9900.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.MT103---USD42880.45---20201127--dbs--9900.exe.4c50000.8.unpack	100%	Avira	TR/Hijacker.Gen		Download File
0.2.MT103---USD42880.45---20201127--dbs--9900.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108767		Download File
0.2.MT103---USD42880.45---20201127--dbs--9900.exe.4cc0000.9.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.1.MT103---USD42880.45---20201127--dbs--9900.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.MT103---USD42880.45---20201127--dbs--9900.exe.2590000.2.unpack	100%	Avira	HEUR/AGEN.1108768		Download File

Domains

Source	Detection	Scanner	Label	Link
discord.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://discord.com/V	0%	Avira URL Cloud	safe	
http://https://cdn.discorda	0%	Avira URL Cloud	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://cdn.disc8	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

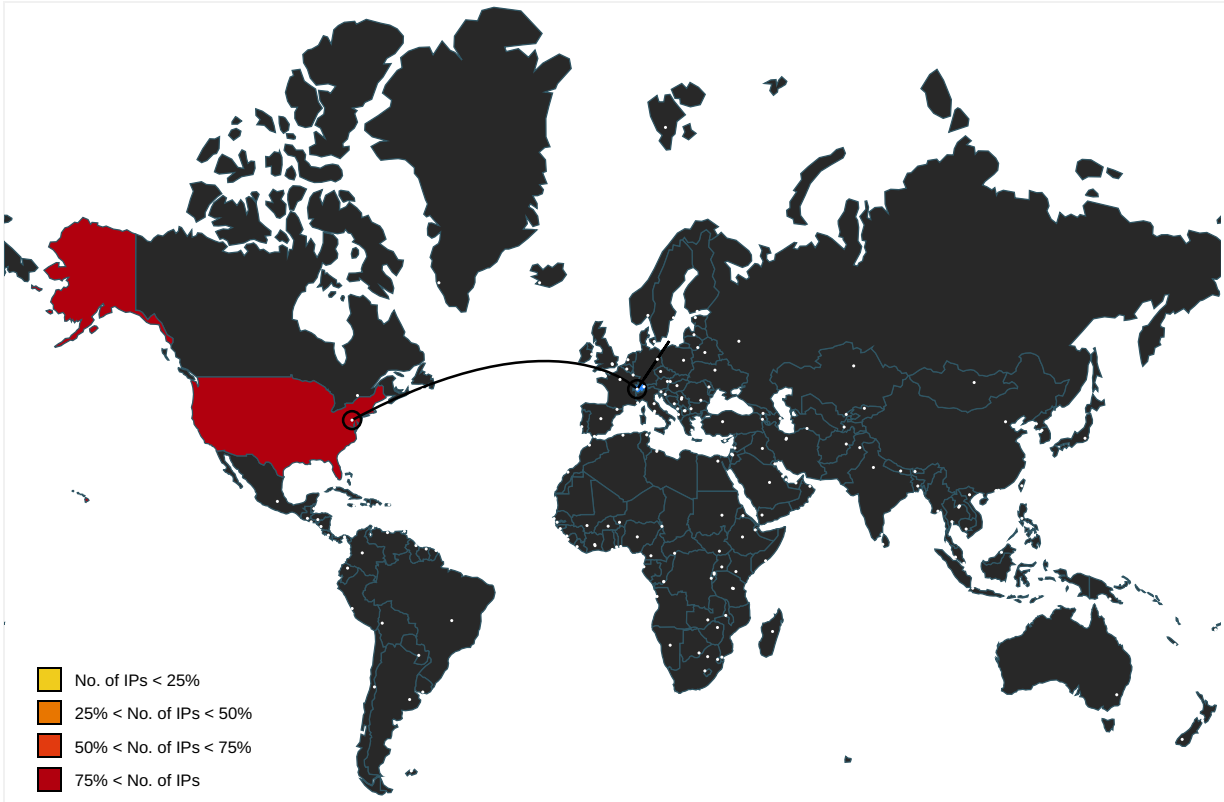
Name	IP	Active	Malicious	Antivirus Detection	Reputation
discord.com	162.159.137.232	true	false	• 1%, Virustotal, Browse	unknown
cdn.discordapp.com	162.159.129.233	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/781839169122205709/781839220499021834/Yipmyyy	MT103---USD42880.45---20201127--dbs--9900.exe, 00000000.00000002.213462989.0000000002E50000.00000004.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attachments/7818391691222	MT103---USD42880.45---20201127--dbs--9900.exe, 00000000.00000002.213462989.0000000002E50000.00000004.00000001.sdmp	false		high
http://https://discord.com/V	MT103---USD42880.45---20201127--dbs--9900.exe, 00000000.00000002.213462989.0000000002E50000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discorda	MT103---USD42880.45---20201127--dbs--9900.exe, 00000000.00000002.213462989.0000000002E50000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/781839169122205709/78183922049902	MT103---USD42880.45---20201127--dbs--9900.exe, 00000000.00000002.213462989.0000000002E50000.00000004.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attac	MT103---USD42880.45---20201127--dbs--9900.exe, 00000000.00000002.213462989.0000000002E50000.00000004.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attachments/781839169122205709	MT103---USD42880.45---20201127--dbs--9900.exe, 00000000.00000002.213462989.0000000002E50000.00000004.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attachments/781839169122205709/7818392204d	MT103---USD42880.45---20201127--dbs--9900.exe, 00000000.00000002.213462989.0000000002E50000.00000004.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attachments/781839169122205709/781839	MT103---USD42880.45---20201127--dbs--9900.exe, 00000000.00000002.213462989.0000000002E50000.00000004.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attachments/7H	MT103---USD42880.45---20201127--dbs--9900.exe, 00000000.00000002.213462989.0000000002E50000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://discord.com/	MT103---USD42880.45---20201127--dbs--9900.exe, 00000000.0000 0002.213462989.0000000002E5000 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn.discordapp.com/attachments/78183	MT103---USD42880.45---20201127--dbs--9900.exe, 00000000.0000 0002.213462989.0000000002E5000 0.00000004.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attachmen	MT103---USD42880.45---20201127--dbs--9900.exe, 00000000.0000 0002.213462989.0000000002E5000 0.00000004.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attachments/781839169122205709/781839220499021834x	MT103---USD42880.45---20201127--dbs--9900.exe, 00000000.0000 0002.213462989.0000000002E5000 0.00000004.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attachments/781839169$	MT103---USD42880.45---20201127--dbs--9900.exe, 00000000.0000 0002.213462989.0000000002E5000 0.00000004.00000001.sdmp	false		high
http://https://cdn.disc8	MT103---USD42880.45---20201127--dbs--9900.exe, 00000000.0000 0002.213462989.0000000002E5000 0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323965
Start date:	28.11.2020

Start time:	00:04:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MT103---USD42880.45---20201127--dbs--9900.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:	2
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:	mal84.troj.evad.winEXE@3/0@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 35.2% (good quality ratio 34%) • Quality average: 71.9% • Quality standard deviation: 29.4%
HCA Information:	• Successful, ratio: 100% • 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 • Stop behavior analysis, all processes terminated
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 13.64.90.137, 168.61.161.212 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, watson.telemetry.microsoft.com • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
00:05:44	API Interceptor	2x Sleep call for process: MT103---USD42880.45---20201127--dbs--9900.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.159.137.232	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	
	tzjEwwwbqK.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	91HN20DCI100053,54,80.exe	Get hash	malicious	Browse	
162.159.129.233	ENQ-015August 2020 R1 Proj LOT.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/722888184203051118/757862128198877274/Stub.jpg

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
discord.com	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
	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
	NyUnwsFSCa.exe	Get hash	malicious	Browse	• 162.159.135.232
	Fl0aIIH39W.exe	Get hash	malicious	Browse	• 162.159.138.232
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	• 162.159.135.232
	9PimjI3jyq.exe	Get hash	malicious	Browse	• 162.159.138.232
	D6vy84I7rJ.exe	Get hash	malicious	Browse	• 162.159.135.232
cdn.discordapp.com	Vessel details.doc	Get hash	malicious	Browse	• 162.159.135.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	9Pimjl3jyq.exe	Get hash	malicious	Browse	• 162.159.133.233
	D6vy84I7rJ.exe	Get hash	malicious	Browse	• 162.159.135.233
	Payment copy.doc	Get hash	malicious	Browse	• 162.159.129.233

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	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
	380000_USD_INV_011740_NOV_2020.jar	Get hash	malicious	Browse	• 104.20.23.46
	http://https://tinyurl.com/y9xs2oe6	Get hash	malicious	Browse	• 104.20.138.65
	case.2522.xls	Get hash	malicious	Browse	• 104.31.87.113
	http://https://ch1.amorozon.fr/.zz?&78387439&user=jon.parr@syngenta.com	Get hash	malicious	Browse	• 104.27.129.197
	case.2522.xls	Get hash	malicious	Browse	• 104.31.87.113
	coinomi-1.20.0.apk	Get hash	malicious	Browse	• 162.159.200.1
	Purchase Order.exe	Get hash	malicious	Browse	• 172.67.143.180
	http://fonts.mafia-server.net	Get hash	malicious	Browse	• 104.18.40.210
	caw.exe	Get hash	malicious	Browse	• 162.159.138.232
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 104.16.19.94
CLOUDFLARENETUS	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	380000_USD_INV_011740_NOV_2020.jar	Get hash	malicious	Browse	• 104.20.23.46
	http://https://tinyurl.com/y9xs2oe6	Get hash	malicious	Browse	• 104.20.138.65
	case.2522.xls	Get hash	malicious	Browse	• 104.31.87.113
	http://https://ch1.amorozon.fr/.zz?&78387439&user=jon.parr@syngenta.com	Get hash	malicious	Browse	• 104.27.129.197
	case.2522.xls	Get hash	malicious	Browse	• 104.31.87.113
	coinomi-1.20.0.apk	Get hash	malicious	Browse	• 162.159.200.1
	Purchase Order.exe	Get hash	malicious	Browse	• 172.67.143.180
	http://fonts.mafia-server.net	Get hash	malicious	Browse	• 104.18.40.210
	caw.exe	Get hash	malicious	Browse	• 162.159.138.232
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 104.16.19.94

JA3 Fingerprints

No context

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):	7.171493979360729
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:	MT103---USD42880.45---20201127--dbs--9900.exe
File size:	1289728
MD5:	d7545487bde794de42b3a655f3664c8d
SHA1:	f4728d4c214b0282efc7d0779cd673d4b68e7da0
SHA256:	4d39dfd975de3e9aca4e430390618b2e548db3f3d4bf2d0409f643be7da2a91e
SHA512:	7d4d4ec5c0aaca0c51f1313769c74428a6615d6919392465ce10a357d81480dd4f80cc6c9c5d7b9d1e5dfe24ed5d6eb152e3e194d50ef81c2fd105768ea676af
SSDEEP:	24576:siLDfJXRq+fowpGG7By3Z72mwt8gKmX9hIbEIK:siLr5By3Z7NTgKA
File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... .....

File Icon

Icon Hash:	b2a8949ea686da6a

Static PE Info

General

Entrypoint:	0x47d118
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, 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
Subsystem Version Minor:	0
Import Hash:	c7f986b767e22dea5696886cb4d7da70

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 0047CE60h
call 00007F2CF4BE5CB5h
lea edx, dword ptr [ebx+eax]
push 00000019h
mov eax, dword ptr [004807A4h]
mov eax, dword ptr [eax]
call 00007F2CF4C3AE08h
mov ecx, dword ptr [00480750h]
mov eax, dword ptr [004807A4h]
mov eax, dword ptr [eax]
mov edx, dword ptr [0047C9ECh]
call 00007F2CF4C3AE08h
mov eax, dword ptr [00480750h]
mov eax, dword ptr [eax]
xor edx, edx
call 00007F2CF4C3437Ah
mov eax, dword ptr [004807A4h]
mov eax, dword ptr [eax]
mov byte ptr [eax+5Bh], 00000000h
mov eax, dword ptr [004807A4h]
mov eax, dword ptr [eax]
call 00007F2CF4C3AE63h
call 00007F2CF4BE37A6h
nop
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
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	0x83000	0x22b0	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x91000	0xb1400	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	0x8138	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x87000	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	0x7c17c	0x7c200	False	0.522454053374	data	6.55138199518	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
DATA	0x7e000	0x2954	0x2a00	False	0.412109375	data	4.92006813937	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x81000	0x114d	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x83000	0x22b0	0x2400	False	0.355251736111	data	4.85312153514	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x86000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x87000	0x18	0x200	False	0.05078125	data	0.206920017787	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x88000	0x8138	0x8200	False	0.584435096154	data	6.65713214053	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x91000	0xb1400	0xb1400	False	0.549854273184	data	7.13542941406	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x9217c	0x134	data		
RT_CURSOR	0x922b0	0x134	data		
RT_CURSOR	0x923e4	0x134	data		
RT_CURSOR	0x92518	0x134	data		
RT_CURSOR	0x9264c	0x134	data		
RT_CURSOR	0x92780	0x134	data		
RT_CURSOR	0x928b4	0x134	data		
RT_BITMAP	0x929e8	0x1d0	data		
RT_BITMAP	0x92bb8	0x1e4	data		
RT_BITMAP	0x92d9c	0x1d0	data		
RT_BITMAP	0x92f6c	0x1d0	data		
RT_BITMAP	0x9313c	0x1d0	data		
RT_BITMAP	0x9330c	0x1d0	data		
RT_BITMAP	0x934dc	0x1d0	data		
RT_BITMAP	0x936ac	0x1d0	data		
RT_BITMAP	0x9387c	0x1d0	data		
RT_BITMAP	0x93a4c	0x1d0	data		
RT_BITMAP	0x93c1c	0x5c	data		
RT_BITMAP	0x93c78	0x5c	data		
RT_BITMAP	0x93cd4	0x5c	data		
RT_BITMAP	0x93d30	0x5c	data		
RT_BITMAP	0x93d8c	0x5c	data		
RT_BITMAP	0x93de8	0x138	data		
RT_BITMAP	0x93f20	0x138	data		
RT_BITMAP	0x94058	0x138	data		
RT_BITMAP	0x94190	0x138	data		
RT_BITMAP	0x942c8	0x138	data		
RT_BITMAP	0x94400	0x138	data		
RT_BITMAP	0x94538	0x104	data		
RT_BITMAP	0x9463c	0x138	data		
RT_BITMAP	0x94774	0x104	data		
RT_BITMAP	0x94878	0x138	data		
RT_BITMAP	0x949b0	0xe8	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x94a98	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x94f00	0x988	data	English	United States
RT_ICON	0x95888	0x10a8	data	English	United States
RT_ICON	0x96930	0x25a8	data	English	United States
RT_ICON	0x98ed8	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	0x9d100	0x5488	data	English	United States
RT_ICON	0xa2588	0x94a8	data	English	United States
RT_ICON	0xaba30	0xa2a8	data	English	United States
RT_DIALOG	0xb5cd8	0x52	data		
RT_STRING	0xb5d2c	0x280	data		

Name	RVA	Size	Type	Language	Country
RT_STRING	0xb5fac	0x274	data		
RT_STRING	0xb6220	0x1ec	data		
RT_STRING	0xb640c	0x13c	data		
RT_STRING	0xb6548	0x2c8	data		
RT_STRING	0xb6810	0xfc	Hitachi SH big-endian COFF object file, not stripped, 17664 sections, symbol offset=0x65007200, 83907328 symbols, optional header size 28672		
RT_STRING	0xb690c	0xf8	data		
RT_STRING	0xb6a04	0x128	data		
RT_STRING	0xb6b2c	0x468	data		
RT_STRING	0xb6f94	0x37c	data		
RT_STRING	0xb7310	0x39c	data		
RT_STRING	0xb76ac	0x3e8	data		
RT_STRING	0xb7a94	0xf4	data		
RT_STRING	0xb7b88	0xc4	data		
RT_STRING	0xb7c4c	0x2c0	data		
RT_STRING	0xb7f0c	0x478	data		
RT_STRING	0xb8384	0x3ac	data		
RT_STRING	0xb8730	0x2d4	data		
RT_RCDATA	0xb8a04	0x10	data		
RT_RCDATA	0xb8a14	0x398	data		
RT_RCDATA	0xb8dac	0x494	Delphi compiled form 'TLoginDialog'		
RT_RCDATA	0xb9240	0x3c4	Delphi compiled form 'TPasswordDialog'		
RT_RCDATA	0xb9604	0x76f67	GIF image data, version 89a, 577 x 188	English	United States
RT_RCDATA	0x13056c	0x11a42	Delphi compiled form 'T__958758541'		
RT_GROUP_CURSOR	0x141fb0	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x141fc4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x141fd8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x141fec	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x142000	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x142014	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0x142028	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0x14203c	0x76	data	English	United States
RT_MANIFEST	0x1420b4	0x2f0	XML 1.0 document, ASCII text, with CRLF line terminators	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, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA

DLL	Import
gdi32.dll	UnrealizeObject, StretchBlt, SetWindowOrgEx, SetWinMetaFileBits, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SelectClipRgn, SaveDC, RestoreDC, Rectangle, RectVisible, RealizePalette, Polyline, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetROP2, GetPolyFillMode, GetPixel, GetPaletteEntries, GetObjectA, GetMapMode, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, GdiFlush, ExcludeClipRect, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt
user32.dll	CreateWindowExA, WindowFromPoint, WinHelpA, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OffsetRect, OemToCharA, MessageBoxA, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, 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, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, 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_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_SetImageCount, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create, InitCommonControls

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 49

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 00:05:45.428303957 CET	49714	443	192.168.2.3	162.159.137.232
Nov 28, 2020 00:05:45.444849014 CET	443	49714	162.159.137.232	192.168.2.3
Nov 28, 2020 00:05:45.445030928 CET	49714	443	192.168.2.3	162.159.137.232
Nov 28, 2020 00:05:45.445923090 CET	49714	443	192.168.2.3	162.159.137.232
Nov 28, 2020 00:05:45.462764978 CET	443	49714	162.159.137.232	192.168.2.3
Nov 28, 2020 00:05:45.463264942 CET	443	49714	162.159.137.232	192.168.2.3
Nov 28, 2020 00:05:45.463382006 CET	49714	443	192.168.2.3	162.159.137.232
Nov 28, 2020 00:05:45.543860912 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.560765982 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.560965061 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.571419954 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.587831974 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.588376045 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.588417053 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.588447094 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.588498116 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.635109901 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.638703108 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.655452013 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.655683994 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.697613955 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.738403082 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.754874945 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.779589891 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.779622078 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.779649019 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.779668093 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.779695034 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.779728889 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.779758930 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.779793978 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.779798985 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.779833078 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.779869080 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.779874086 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.779906034 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.779932022 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.779958010 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.779980898 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.779988050 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.780008078 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780036926 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780064106 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780076981 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.780091047 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780122995 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780143976 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.780158997 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780190945 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780211926 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.780216932 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780252934 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780287981 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780301094 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.780327082 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780361891 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.780366898 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780411959 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780453920 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780462980 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.780491114 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780518055 CET	443	49715	162.159.129.233	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 00:05:45.780544043 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.780555964 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780582905 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780599117 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.780616045 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780647993 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780689001 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780694008 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.780728102 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780766964 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780797005 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.780805111 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780843019 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780854940 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.780883074 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780910015 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.780915022 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780952930 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.780985117 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.780991077 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.781028986 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.781068087 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.781068087 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.781104088 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.781109095 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.781147003 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.781188011 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.781224966 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.781229973 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.781266928 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.781301975 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.781302929 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.781332970 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.781344891 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.781371117 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.781428099 CET	49715	443	192.168.2.3	162.159.129.233
Nov 28, 2020 00:05:45.781575918 CET	443	49715	162.159.129.233	192.168.2.3
Nov 28, 2020 00:05:45.781610012 CET	443	49715	162.159.129.233	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 00:05:39.377357960 CET	64185	53	192.168.2.3	8.8.8.8
Nov 28, 2020 00:05:39.413207054 CET	53	64185	8.8.8.8	192.168.2.3
Nov 28, 2020 00:05:40.531349897 CET	65110	53	192.168.2.3	8.8.8.8
Nov 28, 2020 00:05:40.566946030 CET	53	65110	8.8.8.8	192.168.2.3
Nov 28, 2020 00:05:41.344980955 CET	58361	53	192.168.2.3	8.8.8.8
Nov 28, 2020 00:05:41.372140884 CET	53	58361	8.8.8.8	192.168.2.3
Nov 28, 2020 00:05:42.388803959 CET	63492	53	192.168.2.3	8.8.8.8
Nov 28, 2020 00:05:42.417777061 CET	53	63492	8.8.8.8	192.168.2.3
Nov 28, 2020 00:05:43.434027910 CET	60831	53	192.168.2.3	8.8.8.8
Nov 28, 2020 00:05:43.465171099 CET	53	60831	8.8.8.8	192.168.2.3
Nov 28, 2020 00:05:44.502682924 CET	60100	53	192.168.2.3	8.8.8.8
Nov 28, 2020 00:05:44.529831886 CET	53	60100	8.8.8.8	192.168.2.3
Nov 28, 2020 00:05:45.299616098 CET	53195	53	192.168.2.3	8.8.8.8
Nov 28, 2020 00:05:45.326739073 CET	53	53195	8.8.8.8	192.168.2.3
Nov 28, 2020 00:05:45.375690937 CET	50141	53	192.168.2.3	8.8.8.8
Nov 28, 2020 00:05:45.402848005 CET	53	50141	8.8.8.8	192.168.2.3
Nov 28, 2020 00:05:45.512635946 CET	53023	53	192.168.2.3	8.8.8.8
Nov 28, 2020 00:05:45.540005922 CET	53	53023	8.8.8.8	192.168.2.3
Nov 28, 2020 00:05:46.103368044 CET	49563	53	192.168.2.3	8.8.8.8
Nov 28, 2020 00:05:46.131063938 CET	53	49563	8.8.8.8	192.168.2.3
Nov 28, 2020 00:05:47.257292032 CET	51352	53	192.168.2.3	8.8.8.8
Nov 28, 2020 00:05:47.293032885 CET	53	51352	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 00:05:50.389448881 CET	59349	53	192.168.2.3	8.8.8.8
Nov 28, 2020 00:05:50.425154924 CET	53	59349	8.8.8.8	192.168.2.3
Nov 28, 2020 00:05:51.466330051 CET	57084	53	192.168.2.3	8.8.8.8
Nov 28, 2020 00:05:51.493590117 CET	53	57084	8.8.8.8	192.168.2.3
Nov 28, 2020 00:05:52.523111105 CET	58823	53	192.168.2.3	8.8.8.8
Nov 28, 2020 00:05:52.558619976 CET	53	58823	8.8.8.8	192.168.2.3
Nov 28, 2020 00:05:53.632405043 CET	57568	53	192.168.2.3	8.8.8.8
Nov 28, 2020 00:05:53.659518957 CET	53	57568	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 28, 2020 00:05:45.375690937 CET	192.168.2.3	8.8.8.8	0x2d18	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Nov 28, 2020 00:05:45.512635946 CET	192.168.2.3	8.8.8.8	0xc863	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 00:05:45.402848005 CET	8.8.8.8	192.168.2.3	0x2d18	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Nov 28, 2020 00:05:45.402848005 CET	8.8.8.8	192.168.2.3	0x2d18	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Nov 28, 2020 00:05:45.402848005 CET	8.8.8.8	192.168.2.3	0x2d18	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Nov 28, 2020 00:05:45.402848005 CET	8.8.8.8	192.168.2.3	0x2d18	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Nov 28, 2020 00:05:45.402848005 CET	8.8.8.8	192.168.2.3	0x2d18	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Nov 28, 2020 00:05:45.540005922 CET	8.8.8.8	192.168.2.3	0xc863	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Nov 28, 2020 00:05:45.540005922 CET	8.8.8.8	192.168.2.3	0xc863	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Nov 28, 2020 00:05:45.540005922 CET	8.8.8.8	192.168.2.3	0xc863	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Nov 28, 2020 00:05:45.540005922 CET	8.8.8.8	192.168.2.3	0xc863	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Nov 28, 2020 00:05:45.540005922 CET	8.8.8.8	192.168.2.3	0xc863	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)

HTTPS Packets

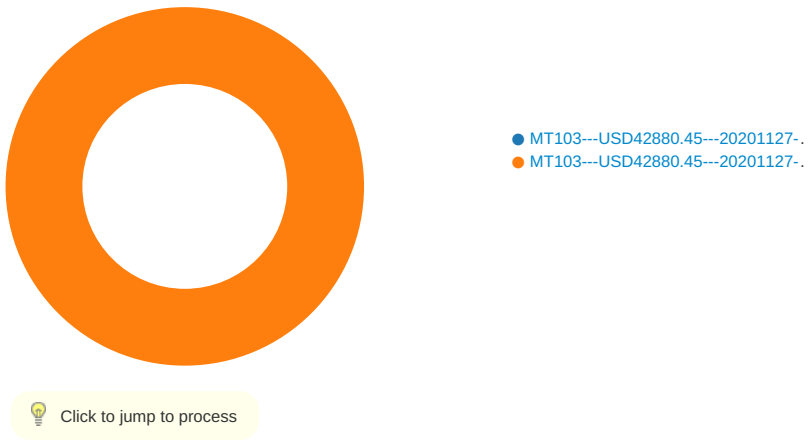
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 28, 2020 00:05:45.588447094 CET	162.159.129.233	443	192.168.2.3	49715	CN=ssl711320.cloudflaressl.com CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=COMODO 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: MT103---USD42880.45---20201127--dbs--9900.exe PID: 5504 Parent PID: 5516

General

Start time:	00:05:43
Start date:	28/11/2020
Path:	C:\Users\user\Desktop\MT103---USD42880.45---20201127--dbs--9900.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\MT103---USD42880.45---20201127--dbs--9900.exe'
Imagebase:	0x400000
File size:	1289728 bytes
MD5 hash:	D7545487BDE794DE42B3A655F3664C8D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000002.214074450.0000000004C67000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000002.214074450.0000000004C67000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.214175689.0000000004CC0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.214175689.0000000004CC0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.214175689.0000000004CC0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.214642043.0000000005126000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.214642043.0000000005126000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.214642043.0000000005126000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: MT103---USD42880.45---20201127--dbs--9900.exe PID: 2416 Parent PID: 5504

General

Start time:	00:05:46
Start date:	28/11/2020
Path:	C:\Users\user\Desktop\MT103---USD42880.45---20201127--dbs--9900.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\MT103---USD42880.45---20201127--dbs--9900.exe
Imagebase:	0x400000
File size:	1289728 bytes
MD5 hash:	D7545487BDE794DE42B3A655F3664C8D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.213378752.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.213378752.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.213378752.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.211862077.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.211862077.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.211862077.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E57	NtReadFile

Disassembly

Code Analysis