ID: 356643
Sample Name:
PO112000891122110.exe
Cookbook: default.jbs
Time: 13:54:10
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

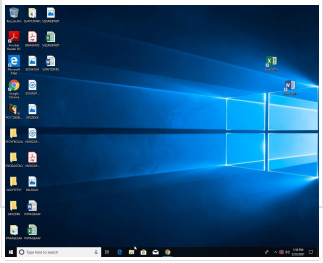
Analysis Report PO1120008911221l0.exe

Overview

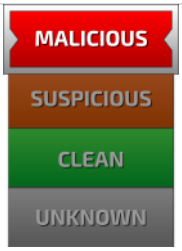
General Information

Sample Name:	PO112000891122110.exe
Analysis ID:	356643
MD5:	fcc9d54e6b6142d..
SHA1:	9be22b91de41b5..
SHA256:	00e8e128207532..
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection



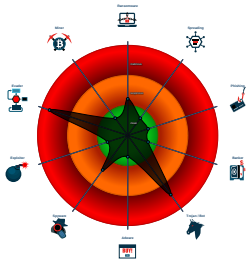
AgentTesla GuLoader

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected GuLoader
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Writes to foreign memory regions
- Checks if the current process is bein…

Classification



Startup

- **System is w10x64**
- PO112000891122110.exe (PID: 5420 cmdline: 'C:\Users\user\Desktop\PO112000891122110.exe' MD5: FCC9D54E6B6142DA1459A6AF8CE507E6)
  - RegAsm.exe (PID: 6820 cmdline: 'C:\Users\user\Desktop\PO112000891122110.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - RegAsm.exe (PID: 6860 cmdline: 'C:\Users\user\Desktop\PO112000891122110.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - RegAsm.exe (PID: 6900 cmdline: 'C:\Users\user\Desktop\PO112000891122110.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - conhost.exe (PID: 6916 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

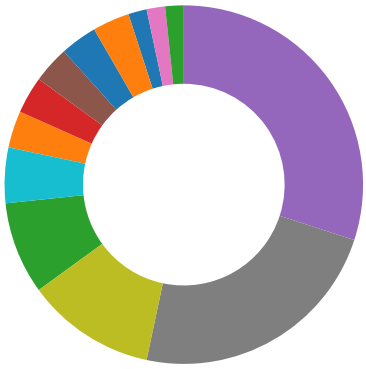
Source	Rule	Description	Author	Strings
0000000C.00000002.482428270.00000000013A1000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
0000000C.00000002.487587781.000000001DF31000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000C.00000002.487587781.000000001DF31000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: RegAsm.exe PID: 6900	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: RegAsm.exe PID: 6900	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 1 entries

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

Uses secure TLS version for HTTPS connections

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

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

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

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

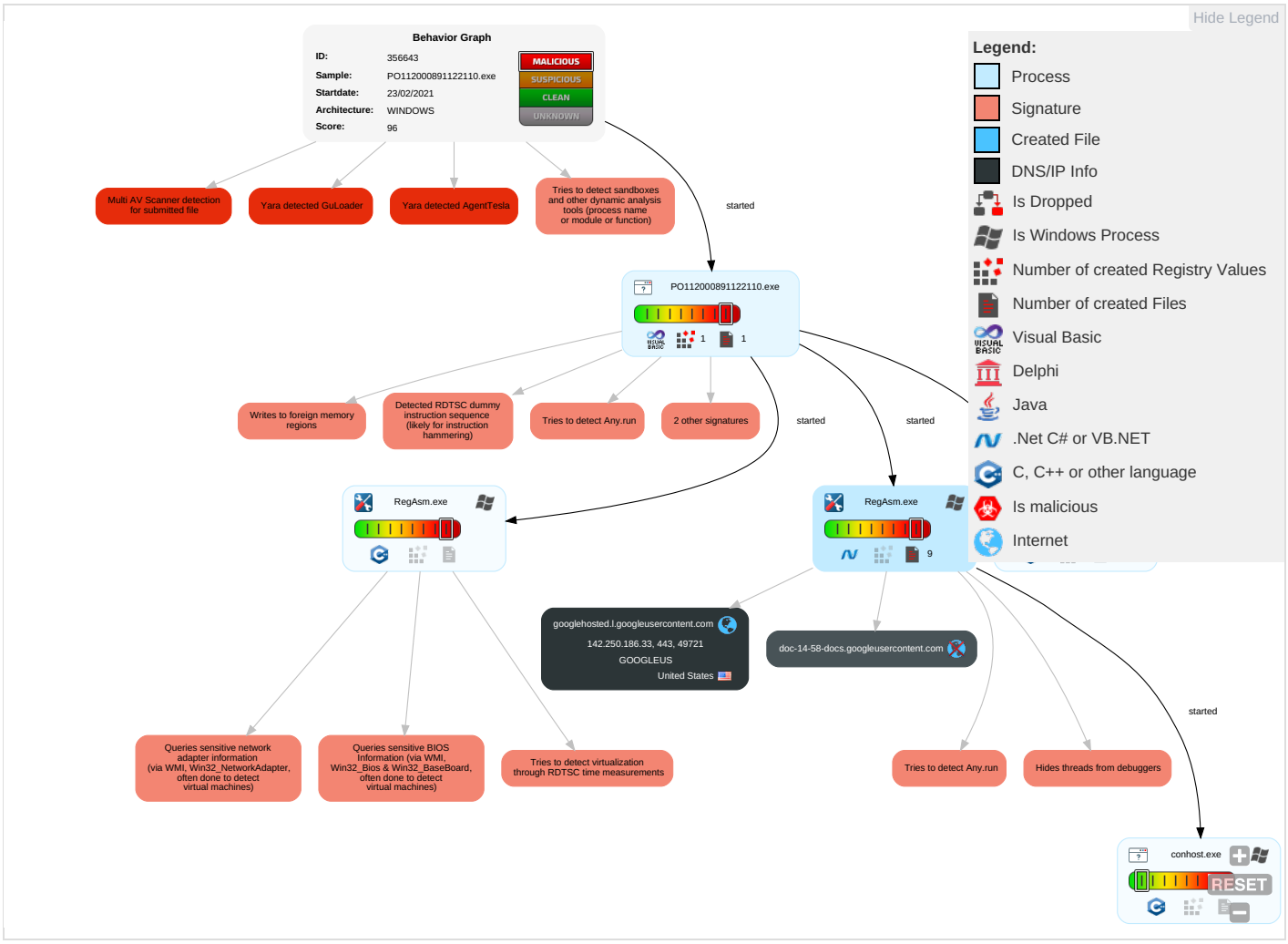
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	Process Injection 1 1 2	Virtualization/Sandbox Evasion 3 4	Input Capture 1	Security Software Discovery 6 3 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	E I N C
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 3 4	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	E F C
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Application Layer Protocol 2	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	N D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 3 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S

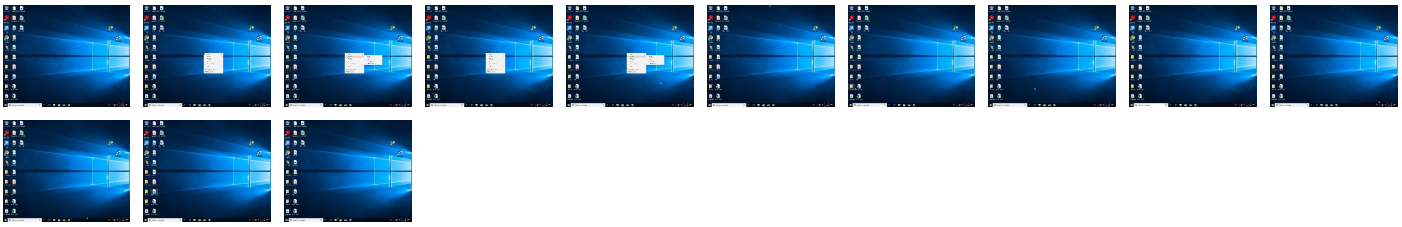
Behavior Graph



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
PO1120008911221 10.exe	48%	Virustotal		Browse
PO1120008911221 10.exe	11%	ReversingLabs	Win32.Worm.Wbvb	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	

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

Domains and IPs

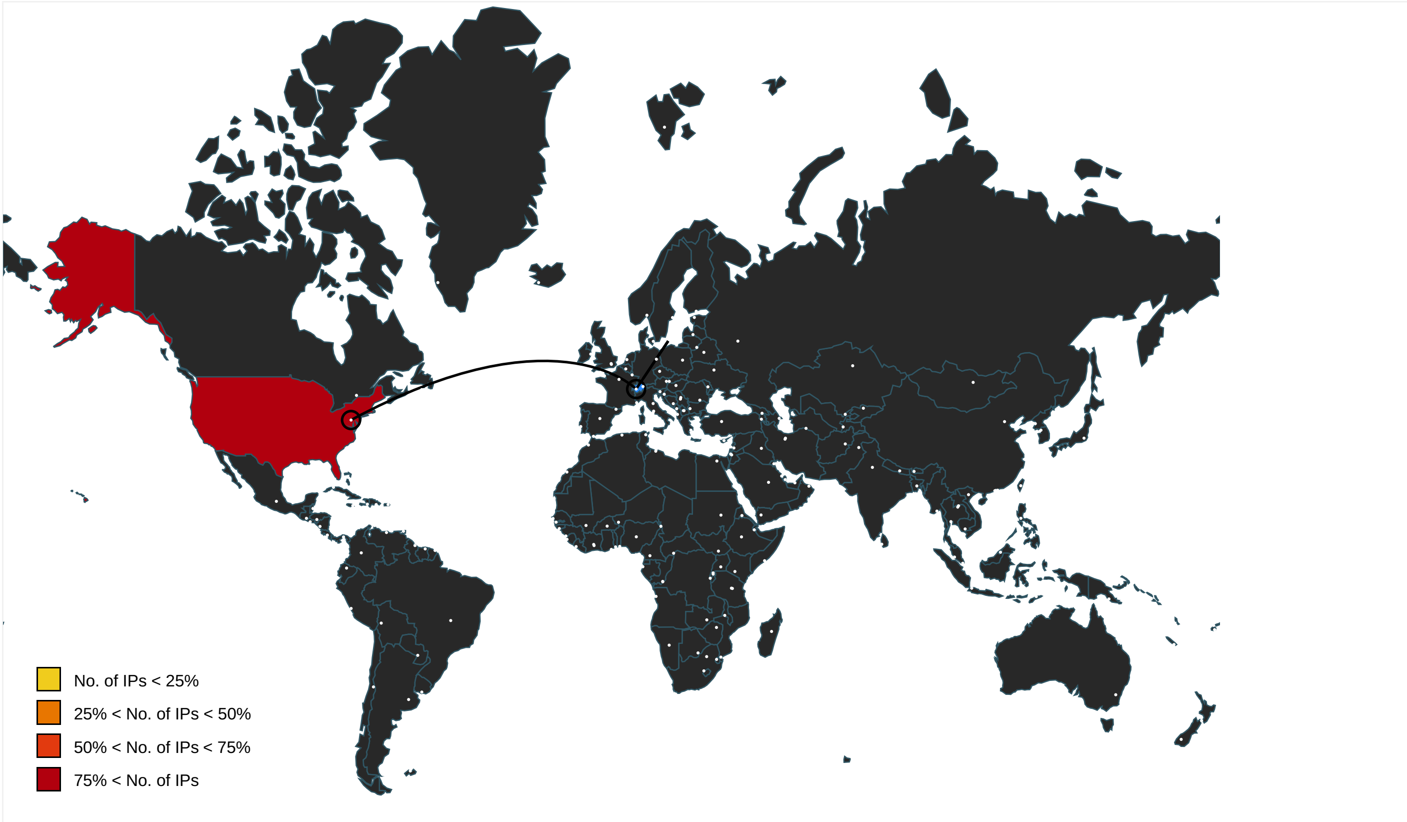
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
googlehosted.l.googleusercontent.com	142.250.186.33	true	false		high
doc-14-58-docs.googleusercontent.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 0000000C.00000002.487587781.000000001DF31000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	RegAsm.exe, 0000000C.00000002.487587781.000000001DF31000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegAsm.exe, 0000000C.00000002.487587781.000000001DF31000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://byztWS.com	RegAsm.exe, 0000000C.00000002.487587781.000000001DF31000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.186.33	unknown	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356643
Start date:	23.02.2021
Start time:	13:54:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO112000891122110.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:	27
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:	mal96.troj.evad.winEXE@8/0@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 46.2% (good quality ratio 22.3%) • Quality average: 32.9% • Quality standard deviation: 37.7%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 204.79.197.200, 13.107.21.200, 93.184.220.29, 51.104.144.132, 104.43.193.48, 13.64.90.137, 23.211.6.115, 168.61.161.212, 13.88.21.125, 23.218.208.56, 216.58.212.174, 51.103.5.159, 51.104.139.180, 93.184.221.240, 92.122.213.194, 92.122.213.247, 20.54.26.129 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, vip1-par02p.wns.notify.trafficmanager.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, drive.google.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:55:50	API Interceptor	535x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
142.250.186.33	GUEROLA INDUSTRIES N#U00ba de cuenta.exe	Get hash	malicious	Browse	
	xerox for hycite.htm	Get hash	malicious	Browse	
	Muligheds.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
googlehosted.l.googleusercontent.com	GUEROLA INDUSTRIES N#U00ba de cuenta.exe	Get hash	malicious	Browse	• 142.250.186.33
	xerox for hycite.htm	Get hash	malicious	Browse	• 142.250.186.33
	Muligheds.exe	Get hash	malicious	Browse	• 142.250.186.33
	2021-Nouvelle masse salariale-Rapport.html	Get hash	malicious	Browse	• 216.58.209.33
	SOLICITUD DE HERJIMAR, SL (HJM-745022821).exe	Get hash	malicious	Browse	• 216.58.208.161
	#U6211#U662f#U56fe#U7247.exe	Get hash	malicious	Browse	• 216.58.208.161
	OneNote rmos@dataflex-int.com.html	Get hash	malicious	Browse	• 216.58.208.129
	Sponsor A Child, Best Online Donation Site, Top NGO - World Vision India.html	Get hash	malicious	Browse	• 172.217.20.225
	barcelona-v-psg-liv-uefa-2021.html	Get hash	malicious	Browse	• 172.217.20.225
	Barcelona-v-PSG-0tv.html	Get hash	malicious	Browse	• 172.217.20.225
	CONSTRUCCIONES SAN MART#U00cdN, S.A. SOLICITAR. (SMT-14517022021).exe	Get hash	malicious	Browse	• 172.217.20.225
	executable.908.exe	Get hash	malicious	Browse	• 216.58.208.161
	executable.908.exe	Get hash	malicious	Browse	• 216.58.208.161
	executable.908.exe	Get hash	malicious	Browse	• 216.58.208.161
	executable.908.exe	Get hash	malicious	Browse	• 216.58.208.161
	OEVGVSOGAH.dll	Get hash	malicious	Browse	• 216.58.206.65
	executable.908.exe	Get hash	malicious	Browse	• 216.58.206.65
	executable.908.exe	Get hash	malicious	Browse	• 216.58.206.65
	executable.908.exe	Get hash	malicious	Browse	• 216.58.206.65
	executable.908.exe	Get hash	malicious	Browse	• 216.58.206.65

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	firefox-3.0.0.zip	Get hash	malicious	Browse	• 35.244.181.201
	MT OCEAN STAR ISO 8217 2005.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	fedex.apk	Get hash	malicious	Browse	• 142.250.18 6.138
	Malody-4.3.7.apk	Get hash	malicious	Browse	• 142.250.186.74
	Malody-4.3.7.apk	Get hash	malicious	Browse	• 142.250.186.42
	Quote_13940007.exe	Get hash	malicious	Browse	• 216.239.32.21
	0O9BJfVJi6fEMoS.exe	Get hash	malicious	Browse	• 34.102.136.180
	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe	Get hash	malicious	Browse	• 34.102.136.180
	dex.dex	Get hash	malicious	Browse	• 142.250.18 5.202
	dex.dex	Get hash	malicious	Browse	• 142.250.18 5.170
	SKBM 0222.exe	Get hash	malicious	Browse	• 216.239.32.21
	lpdKSOB78u.exe	Get hash	malicious	Browse	• 34.102.136.180
	vBugmobiJh.exe	Get hash	malicious	Browse	• 34.102.136.180
	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• 34.102.136.180
	crypted.exe	Get hash	malicious	Browse	• 216.239.32.21
	NewOrder.xlsm	Get hash	malicious	Browse	• 34.102.136.180
	Order_20180218001.exe	Get hash	malicious	Browse	• 34.102.136.180
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	SOA.exe	Get hash	malicious	Browse	• 35.186.238.101
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 34.102.136.180

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	OutplayedInstaller (1).exe	Get hash	malicious	Browse	• 142.250.186.33
	Facecheck - app-Installer (1).exe	Get hash	malicious	Browse	• 142.250.186.33
	Buff-Installer (9).exe	Get hash	malicious	Browse	• 142.250.186.33
	coltTicket#513473.htm	Get hash	malicious	Browse	• 142.250.186.33
	FortPlayerInstaller.exe	Get hash	malicious	Browse	• 142.250.186.33
	RGB HeroInstaller.exe	Get hash	malicious	Browse	• 142.250.186.33
	Buff-Installer.exe	Get hash	malicious	Browse	• 142.250.186.33
	unmapped_executable_of_polyglot_duke.dll	Get hash	malicious	Browse	• 142.250.186.33
	smartandfinalTicket#51347303511505986.htm	Get hash	malicious	Browse	• 142.250.186.33
	f4b1bde3-706a-40d2-8ace-693803810b6f.exe	Get hash	malicious	Browse	• 142.250.186.33
	LIQUIDACION INTERBANCARIA 02_22_2021.xls	Get hash	malicious	Browse	• 142.250.186.33
	document-550193913.xls	Get hash	malicious	Browse	• 142.250.186.33

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	GUEROLA INDUSTRIES N#U00ba de cuenta.exe	Get hash	malicious	Browse	• 142.250.186.33
	receipt145.htm	Get hash	malicious	Browse	• 142.250.186.33
	xerox for hycite.htm	Get hash	malicious	Browse	• 142.250.186.33
	SecuriteInfo.com.Heur.15528.xls	Get hash	malicious	Browse	• 142.250.186.33
	Muligheds.exe	Get hash	malicious	Browse	• 142.250.186.33
	DHL_6368638172 documento de recibo,pdf.exe	Get hash	malicious	Browse	• 142.250.186.33
	PDF.exe	Get hash	malicious	Browse	• 142.250.186.33
	pagamento.exe	Get hash	malicious	Browse	• 142.250.186.33

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):	5.436855505392075
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	PO112000891122110.exe
File size:	73728
MD5:	fcc9d54e6b6142da1459a6af8ce507e6
SHA1:	9be22b91de41b513a1198c9a8b35cec7002b03f0
SHA256:	00e8e1282075324614259944 97ef690fe37b3e1a81df6b001127bfa8ae9036df
SHA512:	504129d03543eaf76e3cd59e7bfe9b8fcc49000e2dd53cdbac2bb0fbbcaa8814fb39597b7cce512956060e9dadf0ff3f8c8211ebc9ac0798b6d8d32274852f3c
SSDEEP:	1536:htDySjFlLM4FUwUbw+TSAQliwYempYID:httLTUwUbwsSAwiwqYI
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D.....=.....Rich.....PE..L....~\V.....0.....@.....

File Icon

Icon Hash:	1e74f2ea62e4a082

Static PE Info

General

Entrypoint:	0x401494
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED

General

DLL Characteristics:	
Time Stamp:	0x565C7E2E [Mon Nov 30 16:49:50 2015 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:	b84199caadebcbcd5f63d7b7de7ff518

Entrypoint Preview

Instruction
push 0040A010h
call 00007FF4E4C62AC3h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
outsb
jmp far 4C00h : 08806E30h
test al, 76h
lahf
inc esi
ror dword ptr [ecx+000028C9h], 00000000h
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+6603038Fh], bl
jne 00007FF4E4C62B3Dh
jnc 00007FF4E4C62B37h
outsb
jnc 00007FF4E4C62AD2h
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
or dword ptr [edi], ebx
xchg eax, ebp
pop es
mov word ptr [ecx-4DBE8BE4h], ss
xor eax, 6367E273h
les ecx, fword ptr [esi]
pop edi
adc eax, 4CCA5E6Dh
xchg dword ptr [ebx+5Ah], ebx
xor al, D3h
pop edi
jne 00007FF4E4C62B0Ch
dec edi
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx

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
or dword ptr [edx+090F0000h], 00000000h
add byte ptr [eax], al
or al, 00h
push edx
inc ebp
push ebx
inc ebp
dec esi
push esp
inc ebp
dec esi
inc ebx
dec ecx
dec esi
inc edi
add byte ptr [56000501h], cl
dec ecx
push esi
inc ecx
push esp
add byte ptr [ecx], bl
add dword ptr [eax], eax
inc edx

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf124	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x12000	0xc24	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x150	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xe6c4	0xf000	False	0.395979817708	data	5.97563810687	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x10000	0x1218	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x12000	0xc24	0x1000	False	0.2666015625	data	2.92316343304	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1237c	0x8a8	data		
RT_GROUP_ICON	0x12368	0x14	data		
RT_VERSION	0x120f0	0x278	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaLenBstr, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaVarForInit, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, __vbaVarTstEq, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, __vbaUI1I2, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, __vbaStrToUnicode, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaErrorOverflow, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaLateMemCall, __vbaStrToAnsi, __vbaVarDup, _CIatan, __vbaStrMove, _allmul, _CItan, __vbaVarForNext, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	Kvikslvbarometer
FileVersion	1.00
CompanyName	Log
ProductName	Log Inverter
ProductVersion	1.00
FileDescription	Log Inverter
OriginalFilename	Kvikslvbarometer.exe

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 67

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 13:55:40.786583900 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:40.835100889 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:40.835263014 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:40.835804939 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:40.884705067 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:40.891868114 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:40.891900063 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:40.891917944 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:40.891935110 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:40.891966105 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:40.892013073 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:40.892019987 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:40.906912088 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:40.955820084 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:40.955981016 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:40.957568884 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.011040926 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.211857080 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.211885929 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.211904049 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.211920977 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.211935043 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.212021112 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.212069035 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.215161085 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.215186119 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.216804028 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.218641996 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.218667030 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.218724012 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.222017050 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.222039938 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.225486994 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.225511074 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.225549936 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.225572109 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.228878975 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.228904963 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.230169058 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.260488033 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.260514975 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.262010098 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.262156963 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.262178898 CET	443	49721	142.250.186.33	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 13:55:41.262250900 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.262273073 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.265535116 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.265561104 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.265634060 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.268960953 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.268986940 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.269144058 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.272420883 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.272448063 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.272563934 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.272603989 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.275863886 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.275897026 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.275983095 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.276026964 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.279277086 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.279304981 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.279422045 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.282690048 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.282718897 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.282804012 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.286025047 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.286050081 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.286137104 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.286159992 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.289155006 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.289180994 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.289275885 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.289295912 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.292256117 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.292279959 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.292372942 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.295392036 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.295416117 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.295520067 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.298465967 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.298491001 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.298624039 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.298661947 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.301604033 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.301626921 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.301779985 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.304716110 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.304738998 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.304810047 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.304836035 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.310363054 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.310385942 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.311448097 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.311474085 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.311661959 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.313211918 CET	49721	443	192.168.2.5	142.250.186.33
Feb 23, 2021 13:55:41.313582897 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.313604116 CET	443	49721	142.250.186.33	192.168.2.5
Feb 23, 2021 13:55:41.313674927 CET	49721	443	192.168.2.5	142.250.186.33

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 13:54:47.978749037 CET	54302	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:54:48.027896881 CET	53	54302	8.8.8.8	192.168.2.5
Feb 23, 2021 13:54:48.129612923 CET	53784	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:54:48.179608107 CET	53	53784	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 13:54:48.200261116 CET	65307	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:54:48.251832962 CET	53	65307	8.8.8.8	192.168.2.5
Feb 23, 2021 13:54:48.282918930 CET	64344	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:54:48.311639071 CET	62060	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:54:48.340244055 CET	53	64344	8.8.8.8	192.168.2.5
Feb 23, 2021 13:54:48.358143091 CET	61805	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:54:48.363409042 CET	53	62060	8.8.8.8	192.168.2.5
Feb 23, 2021 13:54:48.415371895 CET	53	61805	8.8.8.8	192.168.2.5
Feb 23, 2021 13:54:49.301271915 CET	54795	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:54:49.351567030 CET	53	54795	8.8.8.8	192.168.2.5
Feb 23, 2021 13:54:50.899384022 CET	49557	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:54:50.948510885 CET	53	49557	8.8.8.8	192.168.2.5
Feb 23, 2021 13:54:51.020817995 CET	61733	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:54:51.081790924 CET	53	61733	8.8.8.8	192.168.2.5
Feb 23, 2021 13:54:52.346899986 CET	65447	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:54:52.398571968 CET	53	65447	8.8.8.8	192.168.2.5
Feb 23, 2021 13:54:53.901712894 CET	52441	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:54:53.950316906 CET	53	52441	8.8.8.8	192.168.2.5
Feb 23, 2021 13:54:54.932262897 CET	62176	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:54:54.980887890 CET	53	62176	8.8.8.8	192.168.2.5
Feb 23, 2021 13:54:56.290306091 CET	59596	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:54:56.344659090 CET	53	59596	8.8.8.8	192.168.2.5
Feb 23, 2021 13:54:58.102540016 CET	65296	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:54:58.154129982 CET	53	65296	8.8.8.8	192.168.2.5
Feb 23, 2021 13:54:59.536494017 CET	63183	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:54:59.587620020 CET	53	63183	8.8.8.8	192.168.2.5
Feb 23, 2021 13:55:01.207981110 CET	60151	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:55:01.259661913 CET	53	60151	8.8.8.8	192.168.2.5
Feb 23, 2021 13:55:02.427306890 CET	56969	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:55:02.479212046 CET	53	56969	8.8.8.8	192.168.2.5
Feb 23, 2021 13:55:18.612637043 CET	55161	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:55:18.678308964 CET	53	55161	8.8.8.8	192.168.2.5
Feb 23, 2021 13:55:39.823947906 CET	54757	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:55:39.892337084 CET	53	54757	8.8.8.8	192.168.2.5
Feb 23, 2021 13:55:40.713150024 CET	49992	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:55:40.779531956 CET	53	49992	8.8.8.8	192.168.2.5
Feb 23, 2021 13:55:43.009402037 CET	60075	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:55:43.058140039 CET	53	60075	8.8.8.8	192.168.2.5
Feb 23, 2021 13:55:43.082118034 CET	55016	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:55:43.132141113 CET	53	55016	8.8.8.8	192.168.2.5
Feb 23, 2021 13:55:43.466408014 CET	64345	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:55:43.515160084 CET	53	64345	8.8.8.8	192.168.2.5
Feb 23, 2021 13:55:55.655267000 CET	57128	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:55:55.714029074 CET	53	57128	8.8.8.8	192.168.2.5
Feb 23, 2021 13:56:27.064119101 CET	54791	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:56:27.115803957 CET	53	54791	8.8.8.8	192.168.2.5
Feb 23, 2021 13:56:43.267014980 CET	50463	53	192.168.2.5	8.8.8.8
Feb 23, 2021 13:56:43.335036039 CET	53	50463	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 13:55:40.713150024 CET	192.168.2.5	8.8.8.8	0xaff5	Standard query (0)	doc-14-58-docs.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 13:55:40.779531956 CET	8.8.8.8	192.168.2.5	0xaff5	No error (0)	doc-14-58-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 13:55:40.779531956 CET	8.8.8.8	192.168.2.5	0xaff5	No error (0)	googlehosted.l.googleusercontent.com		142.250.186.33	A (IP address)	IN (0x0001)

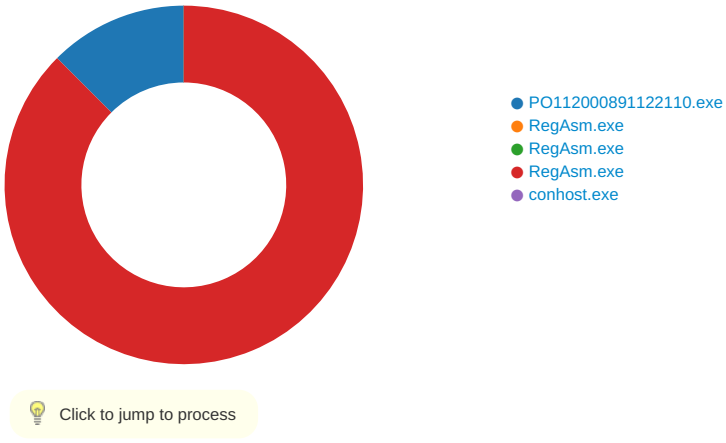
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 13:55:40.891935110 CET	142.250.186.33	443	192.168.2.5	49721	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:05:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:05:01 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PO112000891122110.exe PID: 5420 Parent PID: 5640

General

Start time:	13:54:54
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\PO112000891122110.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\PO112000891122110.exe'
Imagebase:	0x400000
File size:	73728 bytes
MD5 hash:	FCC9D54E6B6142DA1459A6AF8CE507E6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\VB and VBA Program Settings	success or wait	1	660E2872	RegCreateKeyW
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\TANKRENSNING	success or wait	1	660E2872	RegCreateKeyW
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\TANKRENSNING\Sequences	success or wait	1	660E2872	RegCreateKeyW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\TANKRENSNING\Sequences	Koinciderede4	unicode	MS Sans Serif	success or wait	1	660E2183	RegSetValueExW

Analysis Process: RegAsm.exe PID: 6820 Parent PID: 5420

General

Start time:	13:55:30
Start date:	23/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\PO112000891122110.exe'
Imagebase:	0x4e0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 6860 Parent PID: 5420

General

Start time:	13:55:30
Start date:	23/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\PO112000891122110.exe'
Imagebase:	0x490000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 6900 Parent PID: 5420

General

Start time:	13:55:31
Start date:	23/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO112000891122110.exe'
Imagebase:	0xfc0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 0000000C.00000002.482428270.00000000013A1000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.487587781.000000001DF31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.487587781.000000001DF31000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

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	13A2D64	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13A2D64	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13A2D64	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13A2D64	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13A2D64	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13A2D64	InternetOpenUrlA

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	6D2CCF06	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	6D2CCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D2A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D2A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D2A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D2A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D2ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D2ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D2ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D2A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D2A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C111B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C111B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	success or wait	1	6C111B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4096	end of file	1	6C111B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	4095	success or wait	1	6D2A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe.config	unknown	8173	end of file	1	6D2A5705	unknown

Analysis Process: conhost.exe PID: 6916 Parent PID: 6900

General

Start time:	13:55:31
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis