ID: 680378
Sample Name: CSA73881.exe
Cookbook: default.jbs
Time: 14:24:10
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

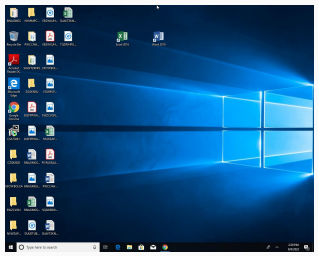
Windows Analysis Report

CSA73881.exe

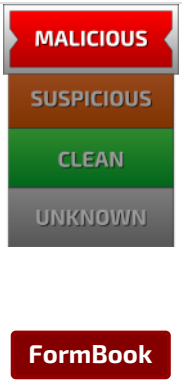
Overview

General Information

Sample Name:	CSA73881.exe
Analysis ID:	680378
MD5:	3ed3236517a406.
SHA1:	16dc042b543fe4..
SHA256:	3702b6cfa76e49..
Tags:	exe formbook
Infos:	



Detection



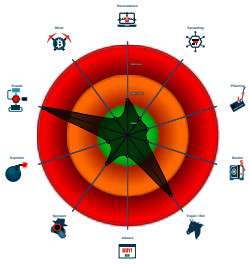
FormBook

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

Signatures

- Yara detected FormBook
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Machine Learning detection for sam…
- Performs DNS queries to domains w…

Classification



Process Tree

- **System is w10x64**
- CSA73881.exe (PID: 5724 cmdline: "C:\Users\user\Desktop\CSA73881.exe" MD5: 3ED3236517A40602D654555BC912D926)
  - InstallUtil.exe (PID: 5408 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
    - explorer.exe (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - control.exe (PID: 3004 cmdline: C:\Windows\SysWOW64\control.exe MD5: 40FBA3FBFD5E33E0DE1BA45472FDA66F)
      - cmd.exe (PID: 2972 cmdline: /c del "C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 3236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.northpierangling.info/mh76/"
  ],
  "decoy": [
    "healthgovcalottery.net",
    "wenxinliao.com",
    "rooterphd.com",
    "bbobbo.one",
    "american-mes-de-dezembro.xyz",
    "mintager.com",
    "thespecialtstore.com",
    "wemakegreenhomes.com",
    "occurandmental.xyz",
    "fidelityrealtytitle.com",
    "numerisat.asia",
    "wearestallions.com",
    "supxl.com",
    "rajacumi.com",
    "renaziv.online",
    "blixtindustries.com",
    "fjljq.com",
    "exploretrivenicamping.com",
    "authenticusspa.com",
    "uucloud.press",
    "conclaveraleighapts.com",
    "moqaq.com",
    "graphicressie.com",
    "homebest.online",
    "yisaco.com",
    "thedrybonesareawakening.com",
    "browardhomeappraisal.com",
    "xn--agroisleos-09a.com",
    "clinchrecovery.com",
    "rekoladev.com",
    "mlbl1.xyz",
    "tunecaring.com",
    "avconstant.com",
    "chelseavictorioustravels.com",
    "esrfy.xyz",
    "frijolitoswey.com",
    "zsfsidltd.com",
    "natashasadler.com",
    "kice1.xyz",
    "drivemytrains.xyz",
    "shopalthosa.xyz",
    "merendri.com",
    "yetkiliveznem7.xyz",
    "milestonesconstruction.com",
    "apparodeoexpos.com",
    "momotou.xyz",
    "chatkhoneh.com",
    "cacconsults.com",
    "kigif-indonesia.com",
    "segurambiental.com",
    "verynicegirls.com",
    "curearrow.com",
    "fdupcoffee.com",
    "theclevergolfers.com",
    "moushimonster.com",
    "qdchuangyedaikuan.com",
    "hopefortodayrecovery.com",
    "wk6agoboyxg6.xyz",
    "giybetfm.com",
    "completedn.xyz",
    "eluawastudio.com",
    "legacysportsusatexas.com",
    "comgmaik.com",
    "intelsearchtech.com"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000000.411747127.000000000D77B000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000010.00000000.411747127.000000000D77B000.00000040.00000001.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x8bc0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x18b7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000010.00000000.411747127.000000000D77B000.00000040.00000001.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x16b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x11a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x17b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x192f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x41c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x7927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x892a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000010.00000000.411747127.000000000D77B000.00000040.00000001.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x4849:$sqlite3step: 68 34 1C 7B E1 • 0x495c:$sqlite3step: 68 34 1C 7B E1 • 0x4878:$sqlite3text: 68 38 2A 90 C5 • 0x499d:$sqlite3text: 68 38 2A 90 C5 • 0x488b:$sqlite3blob: 68 53 D8 7F 8C • 0x49b3:$sqlite3blob: 68 53 D8 7F 8C
0000001C.00000002.765436230.0000000000930000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 32 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
14.0.InstallUtil.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
14.0.InstallUtil.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5451:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1bdc0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x9bcf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x14ab7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
14.0.InstallUtil.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
14.0.InstallUtil.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a49:$sqlite3step: 68 34 1C 7B E1 • 0x17b5c:$sqlite3step: 68 34 1C 7B E1 • 0x17a78:$sqlite3text: 68 38 2A 90 C5 • 0x17b9d:$sqlite3text: 68 38 2A 90 C5 • 0x17a8b:$sqlite3blob: 68 53 D8 7F 8C • 0x17bb3:$sqlite3blob: 68 53 D8 7F 8C
0.2.CSA73881.exe.ee70000.0.raw.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 34.102.136.180

Timestamp:	192.168.2.334.102.136.18049841802031412 08/08/22-14:28:06.715465
SID:	2031412
Source Port:	49841
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 103.224.182.210

Timestamp:	192.168.2.3103.224.182.21049846802031453 08/08/22-14:29:11.618333
SID:	2031453
Source Port:	49846
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 103.224.182.210

Timestamp:	192.168.2.3103.224.182.21049846802031412 08/08/22-14:29:11.618333
SID:	2031412
Source Port:	49846
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 34.102.136.180

Timestamp:	192.168.2.334.102.136.18049841802031449 08/08/22-14:28:06.715465
SID:	2031449
Source Port:	49841
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 103.224.182.210

Timestamp:	192.168.2.3103.224.182.21049846802031449 08/08/22-14:29:11.618333
SID:	2031449
Source Port:	49846
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 34.102.136.180

Timestamp:	192.168.2.334.102.136.18049841802031453 08/08/22-14:28:06.715465
SID:	2031453
Source Port:	49841
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Yara detected FormBook

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking

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

Snort IDS alert for network traffic

Performs DNS queries to domains with low reputation

Yara detected Generic Downloader

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion

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

Writes to foreign memory regions

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

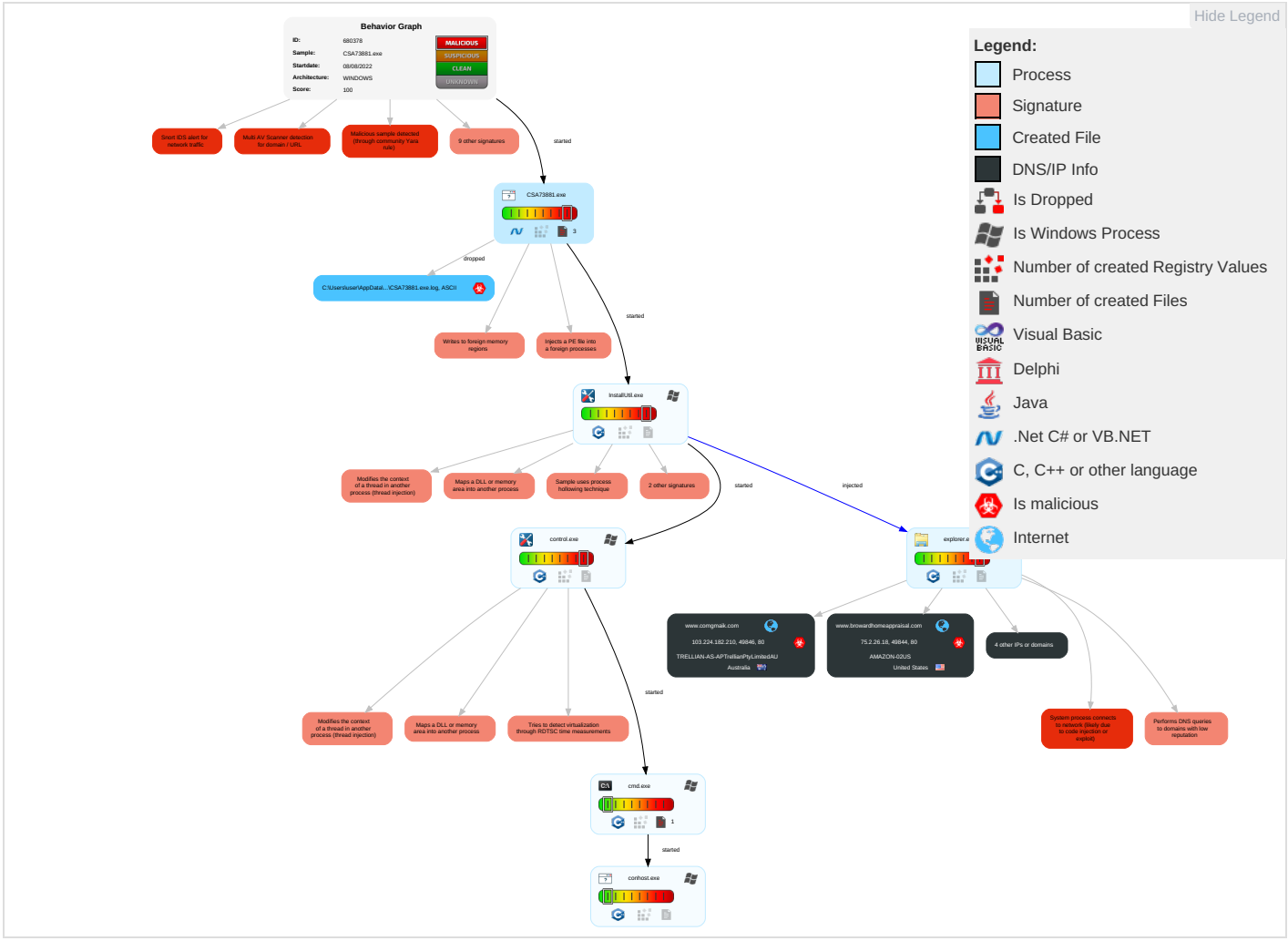
Remote Access Functionality

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	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	Path Interception	7 1 2 Process Injection	1 Rootkit	1 Credential API Hooking	1 2 1 Security Software Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Masquerading	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Disable or Modify Tools	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 Virtualization/Sandbox Evasion	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	7 1 2 Process Injection	LSA Secrets	1 1 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

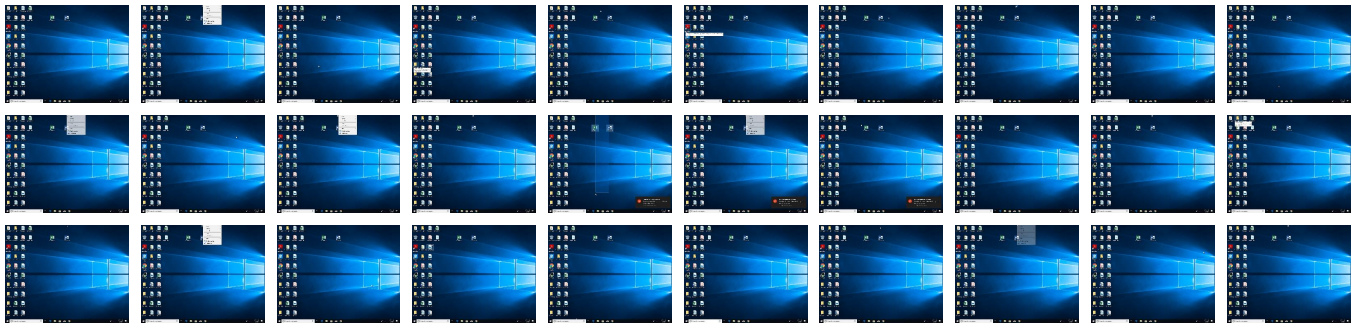
Behavior Graph



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
CSA73881.exe	100%	Avira	HEUR/AGEN.1232160	
CSA73881.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.0.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.0.CSA73881.exe.de0000.0.unpack	100%	Avira	HEUR/AGEN.1232160		Download File

Domains

Source	Detection	Scanner	Label	Link
www.browardhomeappraisal.com	7%	Virustotal		Browse
www.comgmaik.com	2%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
segurambiental.com	9%	Virustotal		Browse
www.segurambiental.com	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.segurambiental.com/mh76/?Axo=j8MnV1AauDvQLYEDQHkxR7wEsLuzS8wOqoRJGUEtb1NYKXHLD1QrWCJCw/4m9jwcj9zX&e0Dd=gPHX06	0%	Avira URL Cloud	safe	
www.northpierangling.info/mh76/	100%	Avira URL Cloud	malware	
http://google.com)Exvkpxtvtblcdcgising7Uvadca.Properties.Resources	0%	Avira URL Cloud	safe	
http://ww38.comgmaik.com/mh76/?Axo=0EXE3m3wBb2Nxgj7DVqNl/WDAC0gNsnNDZKaZxMvJErakGZtakhmesbqHtechaZLz	0%	Avira URL Cloud	safe	
http://www.browardhomeappraisal.com/mh76/?Axo=ZKvJ8T01Uu5swSUTolvzZP3eEu33eLq9PUpXuYL3kSIE+YGu43QnDiKj3vyinvzv5HiX&e0Dd=gPHX06	0%	Avira URL Cloud	safe	
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://www.comgmaik.com/mh76/?Axo=0EXE3m3wBb2Nxgj7DVqNl/WDAC0gNsnNDZKaZxMvJErakGZtakhmesbqHtechaZLzHZ4&e0Dd=gPHX06	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.browardhomeappraisal.com	75.2.26.18	true	true	• 7%, Virustotal, Browse	unknown
www.comgmaik.com	103.224.182.210	true	true	• 2%, Virustotal, Browse	unknown
segurambiental.com	34.102.136.180	true	false	• 9%, Virustotal, Browse	unknown
www.segurambiental.com	unknown	unknown	true	• 6%, Virustotal, Browse	unknown
www.esrfy.xyz	unknown	unknown	true		unknown
www.merendri.com	unknown	unknown	true		unknown

Contacted URLs

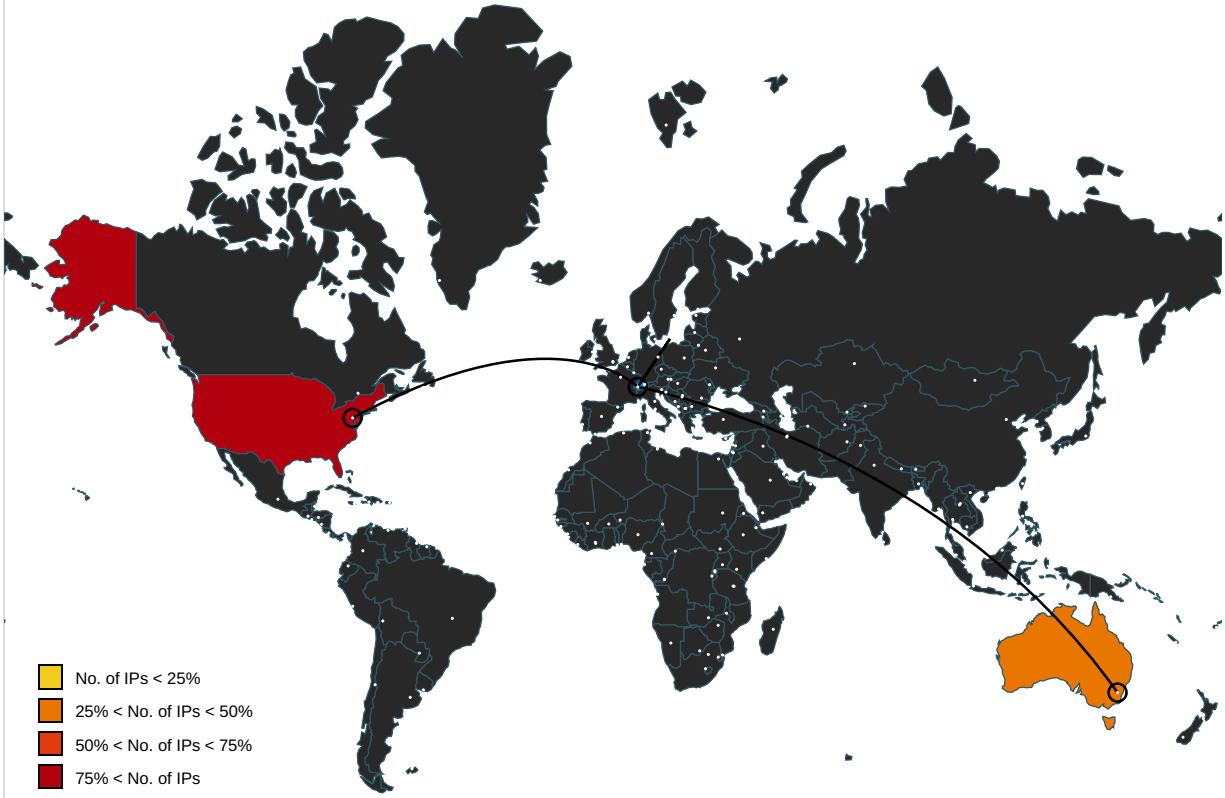
Name	Malicious	Antivirus Detection	Reputation
http://www.segurambiental.com/mh76/?Axo=j8MnV1AauDvQLYEDQHkxR7wEsLuzS8wOqoRJGUEtb1NYKXHLD1QrWCJCw/4m9jwcj9zX&e0Dd=gPHX06	false	• Avira URL Cloud: safe	unknown
www.northpierangling.info/mh76/	true	• Avira URL Cloud: malware	low
http://www.browardhomeappraisal.com/mh76/?Axo=ZKvJ8T01Uu5swSUTolvzZP3eEu33eLq9PUpXuYL3kSIE+YGu43QnDiKj3vyinvzv5HiX&e0Dd=gPHX06	true	• Avira URL Cloud: safe	unknown
http://www.comgmaik.com/mh76/?Axo=0EXE3m3wBb2Nxgj7DVqNl/WDAC0gNsnNDZKaZxMvJErakGZtakhmesbqHtechaZLzHZ4&e0Dd=gPHX06	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.nuget.org/packages/Newtonsoft.Json.Bson	CSA73881.exe, 00000000.00000002.319250218.00000000043F9000.00000004.00000800.00020000.00000000.sdmp, CSA73881.exe, 00000000.00000002.327687009.000000000EE70000.00000004.08000000.00040000.00000000.sdmp	false		high
http://google.com)Exvkpxtvtblcdcgising7Uvadca.Properties.Resources	CSA73881.exe, 00000000.00000000.240713040.0000000000DE2000.00000002.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	low
http://ww38.comgmaik.com/mh76/?Axo=0EXE3m3wBb2Nxgj7DVqNl/WDAC0gNsnNDZKaZxMvJErakGZtakhmesbqHtechaZLz	control.exe, 0000001C.00000002.776382935.00000000056CF000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://google.com	CSA73881.exe, 00000000.00000002.314006871.00000000032B1000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://james.newtonking.com/projects/json	CSA73881.exe, 00000000.00000002.31586097 3.00000000033D0000.00000004.00000800.000 20000.00000000.sdmp, CSA73881.exe, 00000 000.00000002.314521039.00000000032FA000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.newtonsoft.com/jsonschema	CSA73881.exe, 00000000.00000002.31925021 8.00000000043F9000.00000004.00000800.000 20000.00000000.sdmp, CSA73881.exe, 00000 000.00000002.327687009.000000000EE70000. 00000004.08000000.00040000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.102.136.180	segurambiental.com	United States		15169	GOOGLEUS	false
103.224.182.210	www.comgmaik.com	Australia		133618	TRELLIAN-AS-APTrellianPtyLimitedAU	true
75.2.26.18	www.browardhomeappraisal.com	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680378
Start date and time: 08/08/202214:24:10	2022-08-08 14:24:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CSA73881.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:	32
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/1@5/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 93.6% (good quality ratio 81.7%) • Quality average: 71.9% • Quality standard deviation: 33.3%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CSA73881.exe.log

Process:	C:\Users\user\Desktop\CSA73881.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1537
Entropy (8bit):	5.3478589519339295
Encrypted:	false
SSDEEP:	48:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzvFHLHKdHKBqHKs:Pq5qXEwCYqhQnoPtIxHeqzNrqdq4qs
MD5:	F6D3657BD1FBEF54E7F7BACB2497E327
SHA1:	A0A712015C242DCC28B69CDF567F594627C9CFA0
SHA-256:	5B16B4A3E65F04484B12171163A2A739409FA7F8C3D69BF9BAD961618D973301
SHA-512:	0231195A111259A3AA48526DCBEA98394099794C710C3FB8E0E12E2B4D30C60FB4064F7F4F671866FB0D94585E23B73C1270440242B25DA60CCFFA82B0B74306
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.138316897620068
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:	CSA73881.exe
File size:	2187264
MD5:	3ed3236517a40602d654555bc912d926
SHA1:	16dc042b543fe473703e711844f508d353d6d6af
SHA256:	3702b6cfa76e492d56bd9da5f99f7ff805e32c16b3840ee66bb13a812f5d3155
SHA512:	05c6c1d72929e8221522452ce757467a05b07a6e6a8a85ef6f0f16f8dc052068fdb54636f8526dd0eeea7c9fe743dcc4eba6fb84f36cc4a3bbc82b7d057f93d2
SSDEEP:	49152:IYnRpC+ONzKBm/z2DhChFGTbQAbW0S748:lKRpjON1KbZbWH48
TLSH:	48A57C3169562B8B60317CCB841A669FEF717D61DB3240794DB3192B3D228B384FA637
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...g..b.....0..R!.....q!.. .....@.. .....!.....`.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x6171ae
Entrypoint Section:	.text
Digitally signed:	false

Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F0C767 [Mon Aug 8 08:20:55 2022 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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0x217154	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x218000	0xa00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x21a000	0xc	.reloc
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x2151b4	0x215200	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x218000	0xa00	0xa00	False	0.425	data	4.28766916412272	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x21a000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x218100	0x2e8	data		
RT_GROUP_ICON	0x2183f8	0x14	data		
RT_VERSION	0x21841c	0x3a6	data		
RT_MANIFEST	0x2187d4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

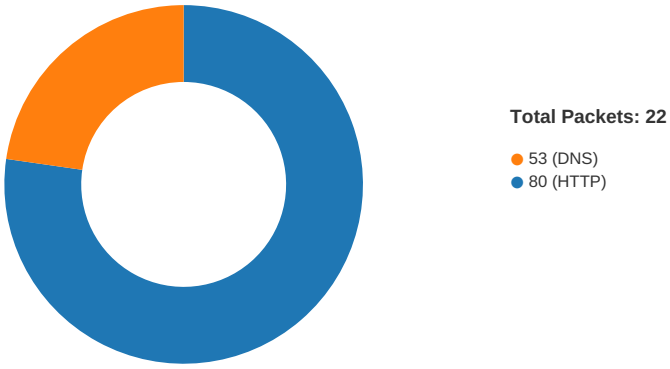
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.334.102.136.18049841802031412 08/08/22-14:28:06.715465	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49841	80	192.168.2.3	34.102.136.180
192.168.2.3103.224.182.21049846802031453 08/08/22-14:29:11.618333	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49846	80	192.168.2.3	103.224.182.210
192.168.2.3103.224.182.21049846802031412 08/08/22-14:29:11.618333	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49846	80	192.168.2.3	103.224.182.210
192.168.2.334.102.136.18049841802031449 08/08/22-14:28:06.715465	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49841	80	192.168.2.3	34.102.136.180

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3103.224.182.21049846802031449 08/08/22-14:29:11.618333	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49846	80	192.168.2.3	103.224.182.210
192.168.2.334.102.136.180498418020314533 08/08/22-14:28:06.715465	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49841	80	192.168.2.3	34.102.136.180

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 14:28:06.695621014 CEST	49841	80	192.168.2.3	34.102.136.180
Aug 8, 2022 14:28:06.714595079 CEST	80	49841	34.102.136.180	192.168.2.3
Aug 8, 2022 14:28:06.714756966 CEST	49841	80	192.168.2.3	34.102.136.180
Aug 8, 2022 14:28:06.715465069 CEST	49841	80	192.168.2.3	34.102.136.180
Aug 8, 2022 14:28:06.734236956 CEST	80	49841	34.102.136.180	192.168.2.3
Aug 8, 2022 14:28:06.831450939 CEST	80	49841	34.102.136.180	192.168.2.3
Aug 8, 2022 14:28:06.831538916 CEST	80	49841	34.102.136.180	192.168.2.3
Aug 8, 2022 14:28:06.831609964 CEST	49841	80	192.168.2.3	34.102.136.180
Aug 8, 2022 14:28:06.831682920 CEST	49841	80	192.168.2.3	34.102.136.180
Aug 8, 2022 14:28:07.143388987 CEST	49841	80	192.168.2.3	34.102.136.180
Aug 8, 2022 14:28:07.160506010 CEST	80	49841	34.102.136.180	192.168.2.3
Aug 8, 2022 14:28:27.360697985 CEST	49844	80	192.168.2.3	75.2.26.18
Aug 8, 2022 14:28:27.379508972 CEST	80	49844	75.2.26.18	192.168.2.3
Aug 8, 2022 14:28:27.382456064 CEST	49844	80	192.168.2.3	75.2.26.18
Aug 8, 2022 14:28:27.382595062 CEST	49844	80	192.168.2.3	75.2.26.18
Aug 8, 2022 14:28:27.401087046 CEST	80	49844	75.2.26.18	192.168.2.3
Aug 8, 2022 14:28:27.562855005 CEST	80	49844	75.2.26.18	192.168.2.3
Aug 8, 2022 14:28:27.562899113 CEST	80	49844	75.2.26.18	192.168.2.3
Aug 8, 2022 14:28:27.563080072 CEST	49844	80	192.168.2.3	75.2.26.18
Aug 8, 2022 14:28:27.563143015 CEST	49844	80	192.168.2.3	75.2.26.18
Aug 8, 2022 14:28:27.577075958 CEST	80	49844	75.2.26.18	192.168.2.3
Aug 8, 2022 14:28:27.578562975 CEST	49844	80	192.168.2.3	75.2.26.18
Aug 8, 2022 14:28:27.581679106 CEST	80	49844	75.2.26.18	192.168.2.3
Aug 8, 2022 14:29:11.449929953 CEST	49846	80	192.168.2.3	103.224.182.210
Aug 8, 2022 14:29:11.616287947 CEST	80	49846	103.224.182.210	192.168.2.3
Aug 8, 2022 14:29:11.618144035 CEST	49846	80	192.168.2.3	103.224.182.210
Aug 8, 2022 14:29:11.618333101 CEST	49846	80	192.168.2.3	103.224.182.210
Aug 8, 2022 14:29:11.821754932 CEST	80	49846	103.224.182.210	192.168.2.3
Aug 8, 2022 14:29:11.822148085 CEST	49846	80	192.168.2.3	103.224.182.210
Aug 8, 2022 14:29:11.822894096 CEST	49846	80	192.168.2.3	103.224.182.210
Aug 8, 2022 14:29:11.988954067 CEST	80	49846	103.224.182.210	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 14:27:44.390386105 CEST	50152	53	192.168.2.3	8.8.8.8
Aug 8, 2022 14:27:44.414792061 CEST	53	50152	8.8.8.8	192.168.2.3
Aug 8, 2022 14:28:06.667161942 CEST	56639	53	192.168.2.3	8.8.8.8
Aug 8, 2022 14:28:06.691601038 CEST	53	56639	8.8.8.8	192.168.2.3
Aug 8, 2022 14:28:27.326817036 CEST	62724	53	192.168.2.3	8.8.8.8
Aug 8, 2022 14:28:27.359499931 CEST	53	62724	8.8.8.8	192.168.2.3
Aug 8, 2022 14:28:48.541207075 CEST	55403	53	192.168.2.3	8.8.8.8
Aug 8, 2022 14:28:48.566221952 CEST	53	55403	8.8.8.8	192.168.2.3
Aug 8, 2022 14:29:11.241316080 CEST	54960	53	192.168.2.3	8.8.8.8
Aug 8, 2022 14:29:11.417627096 CEST	53	54960	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 14:27:44.390386105 CEST	192.168.2.3	8.8.8.8	0x8d48	Standard query (0)	www.merendri.com	A (IP address)	IN (0x0001)
Aug 8, 2022 14:28:06.667161942 CEST	192.168.2.3	8.8.8.8	0xc027	Standard query (0)	www.segurambiental.com	A (IP address)	IN (0x0001)
Aug 8, 2022 14:28:27.326817036 CEST	192.168.2.3	8.8.8.8	0xa489	Standard query (0)	www.browardhomeappraisal.com	A (IP address)	IN (0x0001)
Aug 8, 2022 14:28:48.541207075 CEST	192.168.2.3	8.8.8.8	0x6e44	Standard query (0)	www.esrfy.xyz	A (IP address)	IN (0x0001)
Aug 8, 2022 14:29:11.241316080 CEST	192.168.2.3	8.8.8.8	0x6c24	Standard query (0)	www.comgmaik.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 14:27:44.414792061 CEST	8.8.8.8	192.168.2.3	0x8d48	Name error (3)	www.merendri.com	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 14:28:06.691601038 CEST	8.8.8.8	192.168.2.3	0xc027	No error (0)	www.segurambiental.com	segurambiental.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 14:28:06.691601038 CEST	8.8.8.8	192.168.2.3	0xc027	No error (0)	segurambiental.com		34.102.136.180	A (IP address)	IN (0x0001)
Aug 8, 2022 14:28:27.359499931 CEST	8.8.8.8	192.168.2.3	0xa489	No error (0)	www.browardhomeappraisal.com		75.2.26.18	A (IP address)	IN (0x0001)
Aug 8, 2022 14:28:27.359499931 CEST	8.8.8.8	192.168.2.3	0xa489	No error (0)	www.browardhomeappraisal.com		99.83.153.108	A (IP address)	IN (0x0001)
Aug 8, 2022 14:28:48.566221952 CEST	8.8.8.8	192.168.2.3	0x6e44	Name error (3)	www.esrfy.xyz	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 14:29:11.417627096 CEST	8.8.8.8	192.168.2.3	0x6c24	No error (0)	www.comgmaik.com		103.224.182.210	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.segurambiental.com
- www.browardhomeappraisal.com
- www.comgmaik.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49841	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 14:28:06.715465069 CEST	12256	OUT	GET /mh76/?Axo=j8MnV1AauDvQLYEDQHkxR7wEsLuzS8wOqoRJGUEtb1NYKXHLD1QrWCJCw/4m9jwcj9zX&e0Dd=gPHX06 HTTP/1.1 Host: www.segurambiental.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 14:28:06.831450939 CEST	12256	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 08 Aug 2022 12:28:06 GMT Content-Type: text/html Content-Length: 291 ETag: "62f0fdc3-123" 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 20 20 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 20 2f 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 20 2f 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 20 20 3c 2f 68 65 61 64 3e 0a 20 20 3c 62 6f 64 79 3e 0a 20 20 20 20 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 20 20 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	192.168.2.3	49844	75.2.26.18	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 14:28:27.382595062 CEST	12271	OUT	GET /mh76/?Axo=ZKvJ8T01Uu5swSUTolvzZP3eEu33eLq9PUpXuYL3kSIE+YGu43QnDiKj3vyinvzv5HiX&e0Dd=gPHX06 HTTP/1.1 Host: www.browardhomeappraisal.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 14:28:27.562855005 CEST	12271	IN	HTTP/1.1 403 Forbidden Server: awselb/2.0 Date: Mon, 08 Aug 2022 12:28:27 GMT Content-Type: text/html Content-Length: 118 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49846	103.224.182.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 14:29:11.618333101 CEST	12279	OUT	GET /mh76/?Axo=0EXE3m3wBb2Nxgj7DVqNl/WDAC0gNsnNDZKaZxMvJErakGZtakhmesbqHtechaZLzHZ4&e0Dd=gPHX06 HTTP/1.1 Host: www.comgmaik.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 14:29:11.821754932 CEST	12279	IN	HTTP/1.1 302 Found Date: Mon, 08 Aug 2022 12:29:11 GMT Server: Apache/2.4.38 (Debian) Set-Cookie: __tad=1659961751.8786110; expires=Thu, 05-Aug-2032 12:29:11 GMT; Max-Age=315360000 Location: http://ww38.comgmaik.com/mh76/?Axo=0EXE3m3wBb2Nxgj7DVqNl/WDAC0gNsnNDZKaZxMvJErakGZtakhmesbqHtechaZLzHZ4&e0Dd=gPHX06 Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

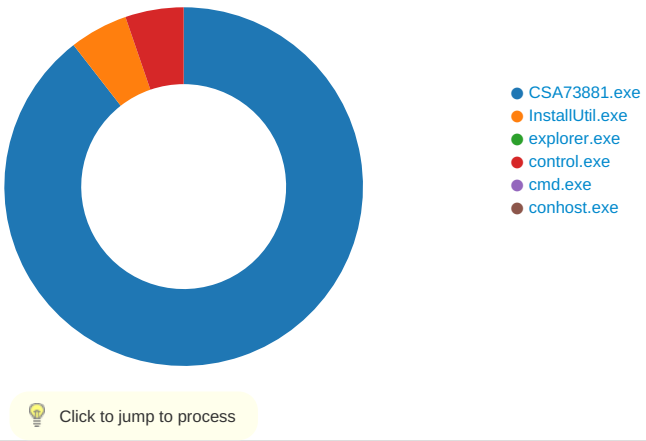
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xED
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xED
GetMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xED
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xED

Statistics

Behavior



System Behavior

Analysis Process: CSA73881.exe PID: 5724, Parent PID: 5252

General

Target ID:	0
Start time:	14:25:09
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\CSA73881.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\CSA73881.exe"
Imagebase:	0xde0000
File size:	2187264 bytes
MD5 hash:	3ED3236517A40602D654555BC912D926
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.315621485.00000000033A4000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.318276189.000000000435E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.318276189.000000000435E000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.318276189.000000000435E000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.318276189.000000000435E000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.319250218.00000000043F9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.319250218.00000000043F9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.319250218.00000000043F9000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.319250218.00000000043F9000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: 00000000.00000002.327687009.000000000EE70000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: InstallUtil.exe PID: **5408**, Parent PID: **5724**

General

Target ID:	14
Start time:	14:25:41
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0x8e0000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
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: 0000000E.00000000.309497191.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000E.00000000.309497191.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000000.309497191.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000000.309497191.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A457	NtReadFile

Analysis Process: explorer.exe PID: **3968**, Parent PID: **5408**

General

Target ID:	16
Start time:	14:25:46
Start date:	08/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE

Imagebase:	0x7ff6b8cf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000000.411747127.000000000D77B000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000010.00000000.411747127.000000000D77B000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000000.411747127.000000000D77B000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000000.411747127.000000000D77B000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000000.390629415.000000000D77B000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000010.00000000.390629415.000000000D77B000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000000.390629415.000000000D77B000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000000.390629415.000000000D77B000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: control.exe PID: **3004**, Parent PID: **5408**

General

Target ID:	28
Start time:	14:26:55
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\control.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\control.exe
Imagebase:	0x890000
File size:	114688 bytes
MD5 hash:	40FBA3FBFD5E33E0DE1BA45472FDA66F
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: 0000001C.00000002.765436230.0000000000930000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000001C.00000002.765436230.0000000000930000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001C.00000002.765436230.0000000000930000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001C.00000002.765436230.0000000000930000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001C.00000002.769483906.0000000002DA0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000001C.00000002.769483906.0000000002DA0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001C.00000002.769483906.0000000002DA0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001C.00000002.769483906.0000000002DA0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001C.00000002.770516120.00000000030A0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000001C.00000002.770516120.00000000030A0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001C.00000002.770516120.00000000030A0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001C.00000002.770516120.00000000030A0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	30BA457	NtReadFile

Analysis Process: cmd.exe PID: **2972**, Parent PID: **3004**

General

Target ID:	29
Start time:	14:27:01
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe"
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **3236**, Parent PID: **2972**

General

Target ID:	30
Start time:	14:27:02
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000

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

No disassembly