ID: 553094
Sample Name: commercial invoice_010202201.exe
Cookbook: default.jbs
Time: 10:19:33
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

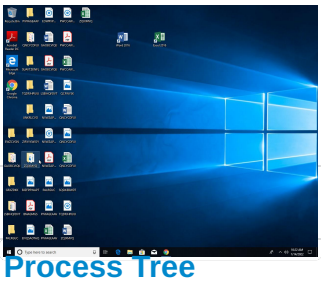
Windows Analysis Report commercial invoice_0102022…

Overview

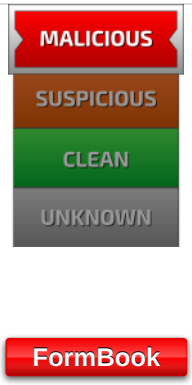
General Information

Sample Name:	commercial invoice_010202201.exe
Analysis ID:	553094
MD5:	acbc7357e4fb7d8..
SHA1:	f423fed0f335e5c…
SHA256:	73f458d7e38ab74.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



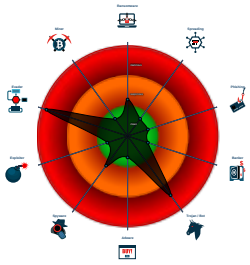
FormBook

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 …
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- commercial invoice_010202201.exe (PID: 5136 cmdline: "C:\Users\user\Desktop\commercial invoice_010202201.exe" MD5: ACBC7357E4FB7D8D4874ECBEB0C5BD0F)
  - commercial invoice_010202201.exe (PID: 2280 cmdline: "C:\Users\user\Desktop\commercial invoice_010202201.exe" MD5: ACBC7357E4FB7D8D4874ECBEB0C5BD0F)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - colorcpl.exe (PID: 5692 cmdline: C:\Windows\SysWOW64\colorcpl.exe MD5: 746F3B5E7652EA0766BA10414D317981)
        - cmd.exe (PID: 2568 cmdline: /c del "C:\Users\user\Desktop\commercial invoice_010202201.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5264 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.toposales.com/igwa/"
  ],
  "decoy": [
    "listingswithalex.com",
    "funtabse.com",
    "aydenwalling.com",
    "prochal.net",
    "superfoodsnederland.com",
    "moldluck.com",
    "dianekgordon.store",
    "regionalhomescommercial.com",
    "mysecuritymadesimple.com",
    "malwaremastery.com",
    "kodaikeiko.com",
    "jrzg996.com",
    "agricurve.net",
    "songlingjiu.com",
    "virginianundahfishingclub.com",
    "friendschance.com",
    "pastelpresents.com",
    "answertitles.com",
    "survival-hunter.com",
    "nxfddl.com",
    "traditionnevertrend.com",
    "agrovessel.com",
    "unicorm.digital",
    "cucumboy.com",
    "alemdogarimpo.com",
    "laraful.com",
    "hexwaa.com",
    "hanu21st.com",
    "knoycia.com",
    "qishengxing.com",
    "gopipurespices.com",
    "fdkkrfidkdslsieofkld.info",
    "elephantspublications.online",
    "valeriebeijing.com",
    "xn--42cg2czax6ptae6a.com",
    "2shengman.com",
    "sfcshavedice.com",
    "ragworkhouse.com",
    "stardomfrokch.xyz",
    "exoticcenterfold.com",
    "eventosartifice.com",
    "test-order-noren.com",
    "110bao.com",
    "face-pro.online",
    "freedomoff.com",
    "futuresep.com",
    "tremblock.com",
    "chocolat-gillotte.com",
    "speclove.com",
    "ddflsl.com",
    "goodnewsmbc.net",
    "cloudtotaal.com",
    "goapps-auth.com",
    "ouch247max.com",
    "sabra-sd.com",
    "luxuryneverhurt.art",
    "rxvendorpills.online",
    "ludowinners.online",
    "placemyorder.online",
    "skyrim.company",
    "monsterlecturer.com",
    "controle-fiscal.com",
    "phoenixinjurylawyer.online",
    "nanoheadgames.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.724210949.000000000EA3D000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000000.724210949.000000000EA3D000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x41a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000000.724210949.000000000EA3D000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x6ad9:$sqlite3step: 68 34 1C 7B E1 • 0x6bec:$sqlite3step: 68 34 1C 7B E1 • 0x6b08:$sqlite3text: 68 38 2A 90 C5 • 0x6c2d:$sqlite3text: 68 38 2A 90 C5 • 0x6b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x6c43:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.943178813.0000000000840000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.943178813.0000000000840000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 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
0.2.commercial invoice_010202201.exe.24d0000.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.commercial invoice_010202201.exe.24d0000.3.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:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.commercial invoice_010202201.exe.24d0000.3.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$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:$sqlite3blob: 68 53 D8 7F 8C
1.1.commercial invoice_010202201.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.commercial invoice_010202201.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$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 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 28 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration
Multi AV Scanner detection for submitted file
Yara detected FormBook
Antivirus detection for URL or domain
Multi AV Scanner detection for dropped file
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)
Performs DNS queries to domains with low reputation
C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)
Initial sample is a PE file and has a suspicious name
Executable has a suspicious name (potential lure to open the executable)

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

Yara detected FormBook

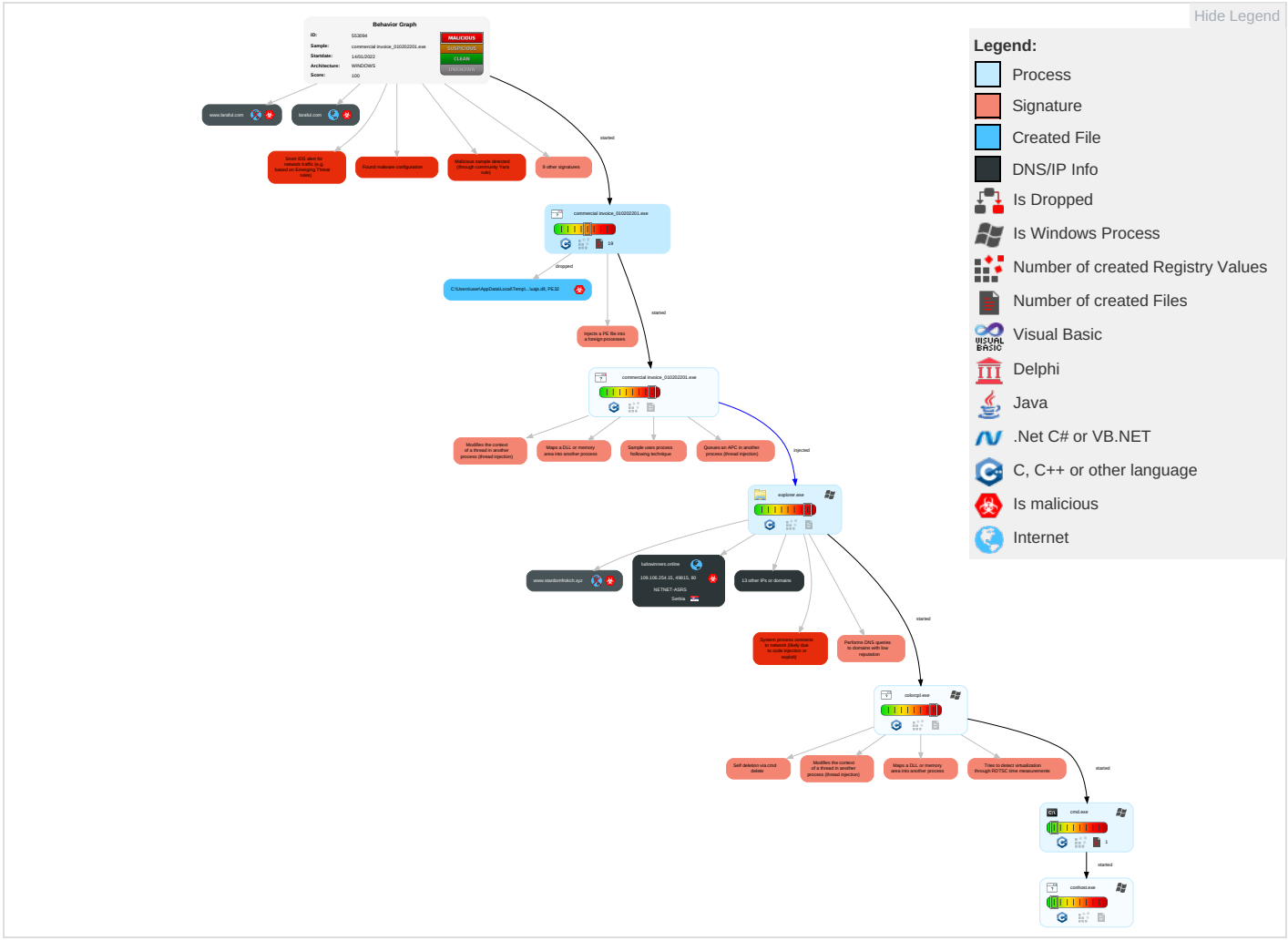
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 6 1 2	Virtualization/Sandbox Evasion 2	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 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 6 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Clipboard 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	Data from Network Shared Drive	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 2	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	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

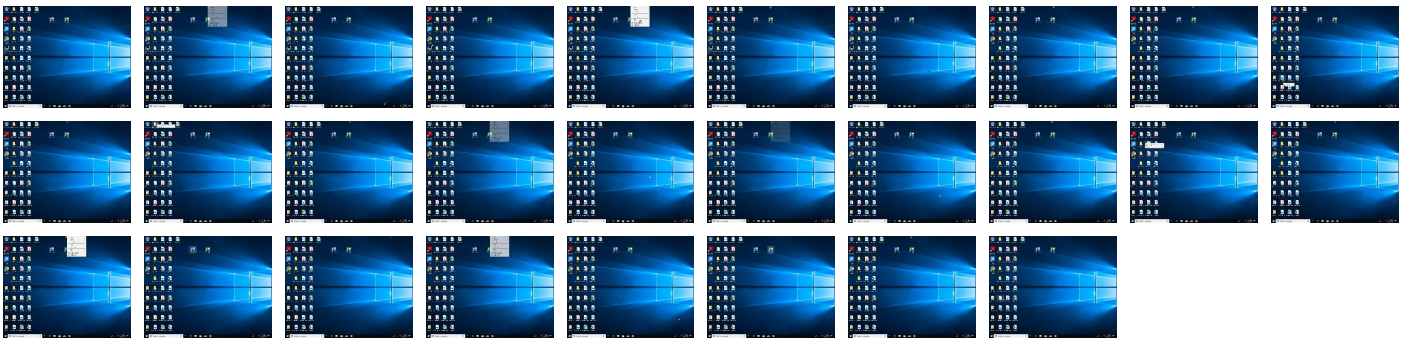
Behavior Graph



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
commercial invoice_010202201.exe	37%	ReversingLabs	Win32.Trojan.Risis	
commercial invoice_010202201.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nshDF13.tmp\uajs.dll	16%	ReversingLabs	Win32.Trojan.Jaik	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.commercial invoice_010202201.exe.24d0000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.colorcpl.exe.b83930.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.commercial invoice_010202201.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
1.0.commercial invoice_010202201.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.1.commercial invoice_010202201.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.commercial invoice_010202201.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.commercial invoice_010202201.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.commercial invoice_010202201.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.colorcpl.exe.4e3796c.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.sfcshavedice.com/igwa/?JXRL2Http=iLZ1RFWiw0U4S9E0pDZlJcjoptUhYXlNWk90HzYHcuVmRCYph1Gowzt+bYvcpjSVMV+b&2dyD8R=k0GL	0%	Avira URL Cloud	safe	
http://www.toposales.com/igwa/?JXRL2Http=ma6dGeieA/uMuLPHhGmEMO0MhvgJCSwWTtOunmNNbuA50fkYJarGKThxl5bT79VqZFZn&2dyD8R=k0GL	100%	Avira URL Cloud	malware	
http://https://www.survival-hunter.com/igwa/?JXRL2Http=XkWoyKtjfo1nTXOdSlOCxSRnTVDbDlQTsKZVtKCHx1ue89AIkDfi	0%	Avira URL Cloud	safe	
http://www.friendschance.com/igwa/?JXRL2Http=kcJK5GFpDKPtevBg1nN4AS2uwE6IDbqQL9Esa69lHd4fhlo3nfdugBZ3P+KHWdbb77iO&2dyD8R=k0GL	0%	Avira URL Cloud	safe	
http://www.ludowinners.online/igwa/?JXRL2Http=P7cOGMhGan+iOds35nuUwcQL6AiWu3hpp80V2Eae8ndsAihNyn6owzlv0a79YI8S4Mj0&2dyD8R=k0GL	0%	Avira URL Cloud	safe	
http://www.survival-hunter.com/igwa/?JXRL2Http=XkWoyKtjfo1nTXOdSlOCxSRnTVDbDlQTsKZVtKCHx1ue89AIkDfi+mwVckT9NwCZj6NC&2dyD8R=k0GL	0%	Avira URL Cloud	safe	
http://www.stardomfrokch.xyz/igwa/?JXRL2Http=fxfNgp9ZS8bh2/dcez9r/a5fPpTZli2HVK4HIQKX3jCJ31NosuhFm2CAaUmyjrkPXZG7&2dyD8R=k0GL	100%	Avira URL Cloud	malware	
www.toposales.com/igwa/	100%	Avira URL Cloud	malware	
http://www.answertitles.com/igwa/?JXRL2Http=zipQeNKESZPqCbLQlDCLj4zpqFgOpmaVmA6du1Oyf7pRL9Y+oEdiiyDWqjEEpcoXahJo&2dyD8R=k0GL	100%	Avira URL Cloud	malware	
http://www.rxvendorpills.online/igwa/?JXRL2Http=pt5DjHHXKdbYY+ulYudT7OdutHPMSBHvoYqZ/+0K/RDZ4aBmJwtpu5HKuc6CLarugF7n&2dyD8R=k0GL	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.friendschance.com	118.67.131.217	true	true		unknown
www.sfcshavedice.com	199.59.243.200	true	true		unknown
www.survival-hunter.com	89.17.204.228	true	true		unknown
parkingpage.namecheap.com	198.54.117.211	true	false		high
laraful.com	34.102.136.180	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
rxvendorpills.online	2.57.90.16	true	true		unknown
ludowinners.online	109.106.254.15	true	true		unknown
www.toposales.com	unknown	unknown	true		unknown
www.ludowinners.online	unknown	unknown	true		unknown
www.cloudtotaal.com	unknown	unknown	true		unknown
www.moldluck.com	unknown	unknown	true		unknown
www.laraful.com	unknown	unknown	true		unknown
www.rxvendorpills.online	unknown	unknown	true		unknown
www.controle-fiscal.com	unknown	unknown	true		unknown
www.answertitles.com	unknown	unknown	true		unknown
www.stardomfrokch.xyz	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.sfcshavedice.com/igwa/?JXRL2Http=iLZ1RFWiw0U4S9E0pDZlJcjoptUhYXlNWk90HzYHcuVmRCYph1Gowzt+bYvcpjSVMV+b&2dyD8R=k0GL	true	• Avira URL Cloud: safe	unknown
http://www.toposales.com/igwa/?JXRL2Http=ma6dGeieA/uMuLPHhGmEMO0MhvgJCSwWTtOunmNNbuA50fkYJarGKThxl5bT79VqZFZn&2dyD8R=k0GL	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.friendschance.com/igwa/?JXRL2Htp=kcJK5GFpDKPtevBg1nN4AS2uwE6IDbqQL9Esa69lHd4fhlo3nfdugBZ3P+KHWdbb77iO&2dyD8R=k0GL	true	• Avira URL Cloud: safe	unknown
http://www.ludowinners.online/igwa/?JXRL2Htp=P7cOGMhGan+iOds35nuUwcQL6AiWu3hpp80V2Eae8ndsAihNyn6owzlv0a79YI8S4Mj0&2dyD8R=k0GL	true	• Avira URL Cloud: safe	unknown
http://www.survival-hunter.com/igwa/?JXRL2Htp=XkWoyKtjfo1nTXOdSlOCxSRnTVDbDlQTsKZVtKCHx1ue89AIkDfi+mwVckT9NwCZj6NC&2dyD8R=k0GL	true	• Avira URL Cloud: safe	unknown
http://www.stardomfrokch.xyz/igwa/?JXRL2Htp=fxfNgp9ZS8bh2/dcez9r/a5fPpTZli2HVK4HIQKX3jCJ31NosuhFm2CAaUmyjrkPXZG7&2dyD8R=k0GL	true	• Avira URL Cloud: malware	unknown
www.toposales.com/igwa/	true	• Avira URL Cloud: malware	low
http://www.answertitles.com/igwa/?JXRL2Htp=zipQeNKESZPqCbLQlDCLj4zpqFgOpmaVmA6du1Oyf7pRL9Y+oEdiiyDWqjEEpcoXahJo&2dyD8R=k0GL	true	• Avira URL Cloud: malware	unknown
http://www.rxvendorpills.online/igwa/?JXRL2Htp=pt5DjHHXKdbYY+ulYudT7OdutHPMSBHvoYqZ/+0K/RDZ4aBmJwtpu5HKuc6CLarugF7n&2dyD8R=k0GL	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
118.67.131.217	www.friendschance.com	Korea Republic of		24395	CLEAR-AS-APClearNetworksPtyLtdAU	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
198.54.117.211	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false
199.59.243.200	www.sfcshavedice.com	United States		395082	BODIS-NJUS	true
2.57.90.16	rxvendorpills.online	Lithuania		47583	AS-HOSTINGERLT	true
109.106.254.15	ludowinners.online	Serbia		199493	NETNET-ASRS	true
89.17.204.228	www.survival-hunter.com	Spain		16371	ACENS_ASSpainHostinghousingandVPNservicesES	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553094
Start date:	14.01.2022
Start time:	10:19:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	commercial invoice_010202201.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:	18
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@14/7
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 56.9% (good quality ratio 51.8%) • Quality average: 72.5% • Quality standard deviation: 31.8%
HCA Information:	• Successful, ratio: 86% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\5kowm48kjaiw3ht	
Process:	C:\Users\user\Desktop\commercial invoice_010202201.exe
File Type:	data
Category:	dropped
Size (bytes):	215764
Entropy (8bit):	**7.9934710763964425**
Encrypted:	**true**
SSDEEP:	6144:EGYAQ1nFCsyFJLgoA7MfkcSCTmhZF7Tr1OvXxj:RvQ1nFCvnwgccSCKhr7PMfp
MD5:	A1416D83EED4E11BA25BBE6EC456D053
SHA1:	467523CD8AA55AC5F208D8B68CD8E660DBBE8C27
SHA-256:	5FFDD6983009916C7C223BED9D3EC43625D2FAA9ACAC5EB77C94EB9E4E0F9B7C
SHA-512:	CD99B3B91FFA401D7B0B63AF71A71258E5C2BBB2F646A519472F7D132B41B6FF4637D9C79429B5B87BB12CD79B20BDBA255543CEBA2C371214485AD94D04489B
Malicious:	false

C:\Users\user\AppData\Local\Temp\5kowm48kjaiw3ht	
Reputation:	low
Preview:	.(...DLJ2/f...^..6pV.z.....w.....-....o.%.%o..(/r..Uq..(...w.....Z-..b.i.....De..*..`.h...:.....p.....t..IXp.}OE..?.q..C2.$..Y.....05_. *Y.....a^....M.....3.GZ2i.....-.;2.;E.f#5E..... .I..F.h.....Wxc:...(. *..._.I.Ni._..=.=.4..[..jr`.DLJ2%...:.i.V"..... .....Y.o.%.%..(/r..Uq..(...h...U.....+.%`._..z.....LP.E.mQ\Cq.a...z..&_F....?.q....i...wC.M.y.....(.....0-D..q. $7.....r..^&2[..f.5E.....R..$.M7.8.....Wxc.K...}(. ...._.I.{i._h.=.=.4..[..j.`.DLJ2'/..e.:.i.V....9.....-....o.%.%o..(/r..Uq..(...h...U.....+.%`._..z.....LP.E.mQ\Cq.a...z..&_F....?.q ....i...wC.M.y.....(.....0-D..q. $7Z2i.....&2[e>.f#5E.....R..$..7.h.....Wxc.K...}(. ...._.I.{i._h.=.=.4..[..j.`.DLJ2'/..e.:.i.V....9.....-....o.%.%o..(/r..Uq..(...h...U.....+.%`._..z.. ....LP.E.mQ\Cq.a...z..&_F....?.q....i...wC.M.y.....(.....0-D..q. $7Z2i.....&2[e>.f#5E.....R..$..7.h.....Wxc.K...}(.

C:\Users\user\AppData\Local\Temp\jfxtaknu	
Process:	C:\Users\user\Desktop\commercial invoice_010202201.exe
File Type:	data
Category:	dropped
Size (bytes):	5330
Entropy (8bit):	6.086371908363251
Encrypted:	false
SSDEEP:	96:RmU+2u9ldYNo8rDVCQq92F6asT6+5biFZ1qqbPimfkDRhlsmI9ltzny:oyo4CQNFc6+9mHPxfkDPQ9ltzny
MD5:	F12ECFF391B1023285050810BDC99341
SHA1:	58BA5DB0B7549E0322C27A4857ED770E19A62E0A
SHA-256:	7D974A756128D4E8D74B20B947684264D6BB6ED85318E53AB78F40E3850642FA
SHA-512:	412D095C737BC53E8C2321FD87962F9AE98D6E9D76A9E4885B197821741DD6007A9445CD6DA28215A7F2895F16BC62037085E5E0101BD174E2E6C051B435F9ED
Malicious:	false
Reputation:	low
Preview:	.xMPP.....+.PE...E1..E...E1...+.P...hPPP.+.P..D..@.....PPP..x..t..D..@.....PPP.....|..D..@.....qPPP.....D..@.....PPP.....@L...H...AA.D.....@..LQ.....L.Qr .@.....A...L.....+.....Q.PPPP.LlKyY+...x....*.....@-..D.-....p..O....x.*..HEK...A+..PPPP..lLaPPP.LlCy.+.....)...DP.....E...E1....H.P..D.p..H.P..@.<.....L.....H.P...H.O .....DP(>J....BPP.&BPP.<P(..u...BPP..BPP.HP(C.....BPP..BPP.HP.....hE...E1.....@PPP..x.....P.>....PP.....<KPP.....H..H...P..Cx..Ct.....H...P..Cx..Ct.B.H...P..Kx.(.. u...OPP.....E.....H.....P.N.+.P.M...OPPP.....LP.....E...E1.....hPPP.....P.>....PP.....!LPP.E.PPP..H..H...P..C...C...D..H...P..C...C...@..H.....C...C...<Q..H*.rA ..;...;.....H...B..C...C..K.H...P..K..(>J....PPP.....8P.H.....8.O.=..8..<..@..D..H.].....P.N.+.P.M...OPPP.....<P.....4...@PPP.....P.>....PP.....APP.....H..H...P. .C...C...D..H...P..C...C..B.H...P..K..(C....mPPP..l.....F..

C:\Users\user\AppData\Local\Temp\nshDF12.tmp	
Process:	C:\Users\user\Desktop\commercial invoice_010202201.exe
File Type:	data
Category:	dropped
Size (bytes):	249957
Entropy (8bit):	7.72387519038227
Encrypted:	false
SSDEEP:	6144:0qGYAQ1nFCsyFJLgoA7MfkcSCTmhZF7Tr1OvXxn:mvQ1nFCvnwgccSCKhr7PMfZ
MD5:	99AB8465F038C2DA8124E3F0F8BD78CE
SHA1:	993EB2793FD14428E5837D9AB2A0B4F42E8CF173
SHA-256:	A67251D5421A9A027B490AB9ED4683BC1370EDD222C7DD2A697511781C75979C
SHA-512:	07D233F8FD0777843AB2A38EC59A679D52C3D638E84D61F20E4D889066B2EC4B5F4E17DDFB81A133133DDA1AA0153E7E24D04CB7B18F8DF6D800AFA52B4924(4
Malicious:	false
Reputation:	low
Preview:	.^.....,.....H.....].....^..... .....J.....j.....-..... ....

C:\Users\user\AppData\Local\Temp\nshDF13.tmp\uajs.dll	
Process:	C:\Users\user\Desktop\commercial invoice_010202201.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	4.170104009362266
Encrypted:	false
SSDEEP:	48:SpotIUM+bADhUYK0JKXIkuW2yH+ZsQMR7/iItlRuqSx:ZtGJDBdJ0FuoH+ZdcZxc
MD5:	85ABDE39747F6B521228F37BE34D4869
SHA1:	8B8F1C057D7369C6FEA384DAF46412F635DDF465
SHA-256:	900E115C271F29C66454E91F168BE012C2AE5D307C86B70E8D595E0BADE388C6
SHA-512:	7F36A7E83FD14924D365845608A9CD76F4ACCB425147E9F12D94A19FF5B50E3D6098E601FE08825AAFEF241B5A4296D7E287CC3FA794DC66C875B19DF850B01
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 16%
Reputation:	low

C:\Users\user\AppData\Local\Temp\nshDF13.tmp\uajs.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x-2..Ca..Ca..CaZ.Ma..Ca..B`..Ca..Ba..Ca.lG`..Ca.lC`..Ca.l.a..Ca.lA`..CaRich..Ca.....PE..L.....a.....!..... .....P.....@..... ..L....!.....0.....@..\..... .....text..... ..`.rdata..l.... .....@..@.rsrc.....0.....@..@.reloc..\....@.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.924746340402354
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:	commercial invoice_010202201.exe
File size:	244072
MD5:	acbc7357e4fb7d8d4874ecbeb0c5bd0f
SHA1:	f423fed0f335e5c31d7b799aba25469420fb6009
SHA256:	73f458d7e38ab748b7b7d3b3e680db9eb08d845c1b1b7c935a6ee453d8f03358
SHA512:	f492401628f2970d3a0056091aea7b7af9938da1d885e0f1a2946f3fed84eb8d132de8f926345791444de7c72c8adbb150d19cd5f81acc8fa1a043d6b0edd17d
SSDEEP:	6144:owJUILHa3T7IFWaZHvyW8od2rrwPs4mAhN4ZY2rB3q:uILHIT7IY4vyW8o6wPs4mAhNORq
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403225
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:	
Time Stamp:	0x48EFCDC9 [Fri Oct 10 21:48:57 2008 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	0x5976	0x5a00	False	0.668619791667	data	6.46680044621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.444878472222	data	5.17796812871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55078125	data	4.68983486809	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	0x900	0xa00	False	0.409375	data	3.94693169534	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
01/14/22-10:22:08.576968	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49817	80	192.168.2.4	198.54.117.211
01/14/22-10:22:08.576968	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49817	80	192.168.2.4	198.54.117.211
01/14/22-10:22:08.576968	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49817	80	192.168.2.4	198.54.117.211
01/14/22-10:22:13.804750	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49839	80	192.168.2.4	23.227.38.74
01/14/22-10:22:13.804750	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49839	80	192.168.2.4	23.227.38.74
01/14/22-10:22:13.804750	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49839	80	192.168.2.4	23.227.38.74
01/14/22-10:22:13.878470	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49839	23.227.38.74	192.168.2.4
01/14/22-10:22:32.377131	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
01/14/22-10:22:33.484922	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
01/14/22-10:22:41.457348	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49846	80	192.168.2.4	34.102.136.180
01/14/22-10:22:41.457348	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49846	80	192.168.2.4	34.102.136.180
01/14/22-10:22:41.457348	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49846	80	192.168.2.4	34.102.136.180
01/14/22-10:22:41.572491	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49846	34.102.136.180	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 10:21:35.349164009 CET	192.168.2.4	8.8.8.8	0x4541	Standard query (0)	www.answertitles.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:21:40.728118896 CET	192.168.2.4	8.8.8.8	0x9d14	Standard query (0)	www.friendschance.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:21:46.791608095 CET	192.168.2.4	8.8.8.8	0x941f	Standard query (0)	www.sfcshavedice.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:21:52.655163050 CET	192.168.2.4	8.8.8.8	0x126	Standard query (0)	www.rxvendorpills.online	A (IP address)	IN (0x0001)
Jan 14, 2022 10:21:57.778915882 CET	192.168.2.4	8.8.8.8	0x9e3b	Standard query (0)	www.ludowinners.online	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:03.240422010 CET	192.168.2.4	8.8.8.8	0x3ce1	Standard query (0)	www.controle-fiscal.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:08.382899046 CET	192.168.2.4	8.8.8.8	0xa528	Standard query (0)	www.stardomfrokch.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:13.762855053 CET	192.168.2.4	8.8.8.8	0x66fd	Standard query (0)	www.toposales.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:18.887667894 CET	192.168.2.4	8.8.8.8	0xfc88	Standard query (0)	www.survival-hunter.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:24.205677032 CET	192.168.2.4	8.8.8.8	0x4a3a	Standard query (0)	www.cloudtotaal.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:29.282247066 CET	192.168.2.4	8.8.8.8	0x80ef	Standard query (0)	www.moldluck.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:30.275973082 CET	192.168.2.4	8.8.8.8	0x80ef	Standard query (0)	www.moldluck.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:31.338468075 CET	192.168.2.4	8.8.8.8	0x80ef	Standard query (0)	www.moldluck.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:41.418489933 CET	192.168.2.4	8.8.8.8	0xd029	Standard query (0)	www.laraful.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 10:20:53.958759069 CET	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a.dns.azurefd.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 10:21:35.373434067 CET	8.8.8.8	192.168.2.4	0x4541	No error (0)	www.answertitles.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 10:21:35.373434067 CET	8.8.8.8	192.168.2.4	0x4541	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 14, 2022 10:21:35.373434067 CET	8.8.8.8	192.168.2.4	0x4541	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 14, 2022 10:21:35.373434067 CET	8.8.8.8	192.168.2.4	0x4541	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 14, 2022 10:21:35.373434067 CET	8.8.8.8	192.168.2.4	0x4541	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 14, 2022 10:21:35.373434067 CET	8.8.8.8	192.168.2.4	0x4541	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 14, 2022 10:21:35.373434067 CET	8.8.8.8	192.168.2.4	0x4541	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 14, 2022 10:21:35.373434067 CET	8.8.8.8	192.168.2.4	0x4541	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 10:21:41.025860071 CET	8.8.8.8	192.168.2.4	0x9d14	No error (0)	www.friendschance.com		118.67.131.217	A (IP address)	IN (0x0001)
Jan 14, 2022 10:21:46.896753073 CET	8.8.8.8	192.168.2.4	0x941f	No error (0)	www.sfcshavedice.com		199.59.243.200	A (IP address)	IN (0x0001)
Jan 14, 2022 10:21:52.688127995 CET	8.8.8.8	192.168.2.4	0x126	No error (0)	www.rxvendorpills.online	rxvendorpills.online		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 10:21:52.688127995 CET	8.8.8.8	192.168.2.4	0x126	No error (0)	rxvendorpills.online		2.57.90.16	A (IP address)	IN (0x0001)
Jan 14, 2022 10:21:57.898154974 CET	8.8.8.8	192.168.2.4	0x9e3b	No error (0)	www.ludowinners.online	ludowinners.online		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 10:21:57.898154974 CET	8.8.8.8	192.168.2.4	0x9e3b	No error (0)	ludowinners.online		109.106.254.15	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:08.406914949 CET	8.8.8.8	192.168.2.4	0xa528	No error (0)	www.stardomfrokch.xyz	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 10:22:08.406914949 CET	8.8.8.8	192.168.2.4	0xa528	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:08.406914949 CET	8.8.8.8	192.168.2.4	0xa528	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:08.406914949 CET	8.8.8.8	192.168.2.4	0xa528	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:08.406914949 CET	8.8.8.8	192.168.2.4	0xa528	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:08.406914949 CET	8.8.8.8	192.168.2.4	0xa528	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:08.406914949 CET	8.8.8.8	192.168.2.4	0xa528	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:08.406914949 CET	8.8.8.8	192.168.2.4	0xa528	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:13.785531044 CET	8.8.8.8	192.168.2.4	0x66fd	No error (0)	www.toposales.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 10:22:13.785531044 CET	8.8.8.8	192.168.2.4	0x66fd	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:19.021996975 CET	8.8.8.8	192.168.2.4	0xfc88	No error (0)	www.survival-hunter.com		89.17.204.228	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:24.233356953 CET	8.8.8.8	192.168.2.4	0x4a3a	Name error (3)	www.cloudtotaal.com	none	none	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:31.391388893 CET	8.8.8.8	192.168.2.4	0x80ef	Server failure (2)	www.moldluck.com	none	none	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:32.377043009 CET	8.8.8.8	192.168.2.4	0x80ef	Server failure (2)	www.moldluck.com	none	none	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:33.484662056 CET	8.8.8.8	192.168.2.4	0x80ef	Server failure (2)	www.moldluck.com	none	none	A (IP address)	IN (0x0001)
Jan 14, 2022 10:22:41.439188004 CET	8.8.8.8	192.168.2.4	0xd029	No error (0)	www.laraful.com	laraful.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 10:22:41.439188004 CET	8.8.8.8	192.168.2.4	0xd029	No error (0)	laraful.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.answertitles.com
- www.friendschance.com
- www.sfcshavedice.com
- www.rxvendorpills.online
- www.ludowinners.online
- www.stardomfrokch.xyz
- www.toposales.com
- www.survival-hunter.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49772	198.54.117.211	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:21:35.543859005 CET	2215	OUT	GET /igwa/?JXRL2Htp=zipQeNKESZPqCbLQlDCLj4zpqFgOpmaVmA6du1Oyf7pRL9Y+oEdiiyDWqjEEpcoXahJo&2dyD8R=k0GL HTTP/1.1 Host: www.answertitles.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49774	118.67.131.217	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:21:41.402209044 CET	2288	OUT	GET /igwa/?JXRL2Htp=kcJK5GFpDKPtevBg1nN4AS2uwE6IDbqQL9Esa69lHd4fhlo3nfdugBZ3P+KHWdbb77iO&2dyD8R=k0GL HTTP/1.1 Host: www.friendschance.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 14, 2022 10:21:41.784310102 CET	2337	IN	HTTP/1.1 302 Found Date: Fri, 14 Jan 2022 09:21:41 GMT P3P: CP="NOI CURa ADMa DEVa TAIa OUR DELa BUS IND PHY ONL UNI COM NAV INT DEM PRE" Location: / Content-Length: 0 Content-Type: text/html; charset=euc-kr Age: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49799	199.59.243.200	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:21:47.487639904 CET	3014	OUT	GET /igwa/?JXRL2Htp=iLZ1RFWiw0U4S9E0pDZlJcjoptUhYXlNWk90HzYHcuVmRCYph1Gowzt+bYvcpjSVMV+b&2dyD8R=k0GL HTTP/1.1 Host: www.sfcshavedice.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:21:47.595983028 CET	3015	IN	HTTP/1.1 200 OK Server: openresty Date: Fri, 14 Jan 2022 09:21:47 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: parking_session=a4e1e271-0068-5577-22f6-a346186a5cf1; expires=Fri, 14-Jan-2022 09:36:47 GMT; Max-Age=900; path=/; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_nX2Kcn56V2Sz7grSVWKurQf0CsgpGLUP6hlKe7ICcjcDdPbUB1bEJDo5qxAmJ9vhByZ21DkHs+CZuvQiBs97PQ== 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 35 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 6e 58 32 4b 63 6e 35 36 56 32 53 7a 37 67 72 53 56 57 4b 75 72 51 66 30 43 73 67 70 47 4c 55 50 36 68 6c 4b 65 37 49 43 63 6a 63 44 64 50 62 55 42 31 62 45 4a 44 6f 35 71 78 41 6d 4a 39 76 68 42 79 5a 32 31 44 6b 48 73 2b 43 5a 75 76 51 69 42 73 39 37 50 51 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 67 6c 65 2e 63 6f 6d 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3e 3c Data Ascii: 585<!doctype html><html lang="en" data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_nX2Kcn56V2Sz7grSVWKurQf0CsgpGLUP6hlKe7ICcjcDdPbUB1bEJDo5qxAmJ9vhByZ21DkHs+CZuvQiBs97PQ=="><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
3	192.168.2.4	49814	2.57.90.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:21:52.729005098 CET	10412	OUT	GET /igwa/?JXRL2Htp=pt5DjHHXKdbYY+ulYudT7OdutHPMSBHvoYqZ/+0K/RDZ4aBmJwtpu5HKuc6CLarugF7n&2dyD8R=k0GL HTTP/1.1 Host: www.rxvendorpills.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 14, 2022 10:21:52.765479088 CET	10412	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 14 Jan 2022 09:21:52 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 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>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49815	109.106.254.15	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:21:58.063568115 CET	10413	OUT	GET /igwa/?JXRL2Htp=P7cOGMhGan+iOds35nuUwcQL6AiWu3hpp80V2Eae8ndsAihNyn6owzlv0a79YI8S4Mj0&2dyD8R=k0GL HTTP/1.1 Host: www.ludowinners.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:21:58.224889040 CET	10415	IN	HTTP/1.1 404 Not Found Connection: close content-type: text/html last-modified: Fri, 26 Mar 2021 09:43:38 GMT etag: "999-605dacca-1fd7389c82cb2d72;;;" accept-ranges: bytes content-length: 2457 date: Fri, 14 Jan 2022 09:21:58 GMT server: LiteSpeed 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 2d 75 73 22 20 70 72 65 66 69 78 3d 22 63 6f 6e 74 65 6e 74 3a 20 68 74 74 70 3a 2f 2f 70 75 72 6c 2e 6f 72 67 2f 72 73 73 2f 31 2e 30 2f 6d 6f 64 75 6c 65 73 2f 63 6f 6e 74 65 6e 74 2f 20 64 63 3a 20 68 74 74 70 3a 2f 2f 70 75 72 6c 2e 6f 72 67 2f 64 63 2f 74 65 72 6d 73 2f 20 66 6f 61 66 3a 20 68 74 74 70 3a 2f 2f 78 6d 6c 6e 73 2e 63 6f 6d 2f 66 6f 61 66 2f 30 2e 31 2f 20 6f 67 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 20 72 64 66 73 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 30 31 2f 72 64 66 2d 73 63 68 65 6d 61 23 20 73 69 6f 63 3a 20 68 74 74 70 3a 2f 2f 72 64 66 73 2e 6f 72 67 2f 73 69 6f 63 2f 6e 73 23 20 73 69 6f 63 74 3a 20 68 74 74 70 3a 2f 2f 72 64 66 73 2e 6f 72 67 2f 73 69 6f 63 2f 74 79 70 65 73 23 20 73 6b 6f 73 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 34 2f 30 32 2f 73 6b 6f 73 2f 63 6f 72 65 23 20 78 73 64 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 23 22 3e 0a 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 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 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 40 63 68 61 72 73 65 74 20 22 55 54 46 2d 38 22 3b 0a 20 20 20 20 20 20 20 20 5b 6e 67 5c 3a 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 5b 6e 67 2d 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 5b 64 61 74 61 2d 6e 67 2d 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 5b 78 2d 6e 67 2d 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 63 6c 6f 61 6b 2c 0a 20 20 20 20 20 20 20 20 2e 78 2d 6e 67 2d 63 6c 6f 61 6b 2c 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 68 69 64 65 3a 6e 6f 74 28 2e 6e 67 2d 68 69 64 65 2d 61 6e 69 6d 61 74 65 29 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 20 20 20 20 6e 67 5c 3a 66 6f 72 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 6e 67 2d 61 6e 69 6d 61 74 65 2d 73 68 69 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 76 69 73 69 62 69 6c 69 74 79 3a 20 68 69 64 64 65 6e 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 61 6e 63 68 6f 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0a 20 20 20 20 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 0a 20 20 20 20 3c 74 69 74 6c 65 3e 4f 6f 70 73 2c 20 73 6f 6d 65 Data Ascii: <!DOCTYPE html><html lang="en-us" prefix="content: http://purl.org/rss/1.0/modules/content/ dc: http://purl.org/dc/terms/ foaf: http://xmlns.com/foaf/0.1/ og: http://ogp.me/ns# rdfs: http://www.w3.org/2000/01/rdf-schema# sioc: http://rdfs.org/sioc/ns# sioct: http://rdfs.org/sioc/types# skos: http://www.w3.org/2004/02/skos/core# xsd: http://www.w3.org/2001/XMLSchema#"><head> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"> <style type="text/css"> @charset "UTF-8"; [ng\:cloak], [ng-cloak], [data-ng-cloak], [x-ng-cloak], .ng-cloak, .x-ng-cloak, .ng-hide:not(.ng-hide-animate) { display: none !important; } ng\:form { display: block; } .ng-animate-shim { visibility: hidden; } .ng-anchor { position: absolute; } </style> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1"> <title>Oops, some

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49817	198.54.117.211	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:22:08.576967955 CET	11071	OUT	GET /igwa/?JXRL2Htp=fxfNgp9ZS8bh2/dcez9r/a5fPpTZli2HVK4HIQKX3jCJ31NosuhFm2CAaUmyjrkPXZG7&2dyD8R=k0GL HTTP/1.1 Host: www.stardomfrokch.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49839	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:22:13.804749966 CET	11120	OUT	GET /igwa/?JXRL2Htp=ma6dGeieA/uMuLPHhGmEMO0MhvgJCSwWTtOunmNNbuA50fkYJarGKThxl5bT79VqZFZn&2dyD8R=k0GL HTTP/1.1 Host: www.toposales.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:22:13.878469944 CET	11123	IN	HTTP/1.1 403 Forbidden Date: Fri, 14 Jan 2022 09:22:13 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 162 X-Sorting-Hat-ShopId: 59837907107 X-Dc: gcp-europe-west1 X-Request-ID: aa596adc-d6ad-4249-95ff-1ddd0936ac81 X-XSS-Protection: 1; mode=block X-Download-Options: noopen X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none CF-Cache-Status: DYNAMIC Server: cloudflare CF-RAY: 6cd5cc745a4f4eda-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":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 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng: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-dec oration: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;displ ay:flex;min-height:100vh;flex-direction:col

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49842	89.17.204.228	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:22:19.083188057 CET	11135	OUT	GET /igwa/?JXRL2Htp=XkWoyKtjfo1nTXOdSlOCxSRnTVDbDlQTsKZVtKCHx1ue89AIkDfi+mwVckT9NwCZj6NC&2dyD8R=k0GL HTTP/1.1 Host: www.survival-hunter.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 14, 2022 10:22:19.142043114 CET	11135	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 14 Jan 2022 09:22:19 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.survival-hunter.com/igwa/?JXRL2Htp=XkWoyKtjfo1nTXOdSlOCxSRnTVDbDlQTsKZVtKCHx1ue89AIkDfi+mwVckT9NwCZj6NC&2dyD8R=k0GL 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>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: commercial invoice_010202201.exe PID: 5136 Parent PID: 4604

General

Start time:	10:20:34
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\commercial invoice_010202201.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\commercial invoice_010202201.exe"
Imagebase:	0x400000
File size:	244072 bytes
MD5 hash:	ACBC7357E4FB7D8D4874ECBEB0C5BD0F
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: 00000000.00000002.684515083.00000000024D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.684515083.00000000024D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.684515083.00000000024D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: commercial invoice_010202201.exe PID: 2280 Parent PID: 5136

General

Start time:	10:20:36
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\commercial invoice_010202201.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\commercial invoice_010202201.exe"
Imagebase:	0x400000
File size:	244072 bytes
MD5 hash:	ACBC7357E4FB7D8D4874ECBEB0C5BD0F
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: 00000001.00000002.734155296.0000000000910000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.734155296.0000000000910000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.734155296.0000000000910000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.683264295.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.683264295.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.683264295.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.734132001.00000000008E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.734132001.00000000008E0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.734132001.00000000008E0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.684056939.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.684056939.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.684056939.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.681309945.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.681309945.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.681309945.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.734016685.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.734016685.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.734016685.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 2280

General

Start time:	10:20:39
Start date:	14/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000005.00000000.724210949.000000000EA3D000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.724210949.000000000EA3D000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.724210949.000000000EA3D000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.708365892.000000000EA3D000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.708365892.000000000EA3D000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.708365892.000000000EA3D000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: colorcpl.exe PID: 5692 Parent PID: 3424

General

Start time:	10:20:59
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\colorcpl.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\colorcpl.exe
Imagebase:	0x1330000
File size:	86528 bytes
MD5 hash:	746F3B5E7652EA0766BA10414D317981
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: 00000007.00000002.943178813.0000000000840000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.943178813.0000000000840000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.943178813.0000000000840000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.943350067.0000000000DF0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.943350067.0000000000DF0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.943350067.0000000000DF0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.943426858.0000000001150000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.943426858.0000000001150000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.943426858.0000000001150000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2568 Parent PID: 5692

General

Start time:	10:21:03
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\commercial invoice_010202201.exe"
Imagebase:	0x11d0000
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: 5264 Parent PID: 2568

General

Start time:	10:21:03
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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