




**ID:** 383640
**Sample Name:**
ensono8639844766FAXMESSAGE.HTM
**Cookbook:**
defaultwindowshtmlcookbook.jbs
**Time:** 04:06:10
**Date:** 08/04/2021
**Version:** 31.0.0 Emerald

# Table of Contents


Table of Contents 2
Analysis Report ensono8639844766FAXMESSAGE.HTM 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
Signature Overview 4
Phishing: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 12
Created / dropped Files 12
Static File Info 17
General 17
Network Behavior 18
Network Port Distribution 18
TCP Packets 18
UDP Packets 19
DNS Queries 21
DNS Answers 21
HTTPS Packets 21
Code Manipulations 23
Statistics 24
Behavior 24
System Behavior 24
Analysis Process: iexplore.exe PID: 5504 Parent PID: 792 24
General 24


Copyright Joe Security LLC 2021

File Activities 24
Registry Activities 24
Analysis Process: iexplore.exe PID: 1156 Parent PID: 5504 25
General 25
File Activities 25
Registry Activities 25
Disassembly 25

Copyright Joe Security LLC 2021

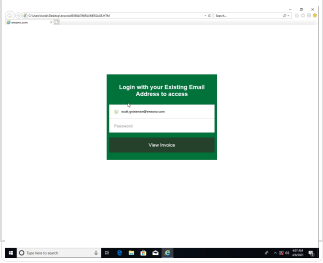
# Analysis Report ensono8639844766FAXMESSAGE.HTM

## Overview

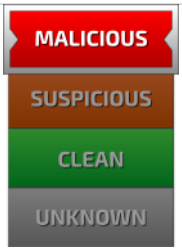
### General Information

| | |
|---|---|
| Sample Name: | ensono8639844766FAXMESSAGE.HTM |
| Analysis ID: | 383640 |
| MD5: | 01606c8d7d638c.. |
| SHA1: | d8860ce2a55d68.. |
| SHA256: | 785bba689dc59c.. |
| Infos: | |

Most interesting Screenshot:



### Detection



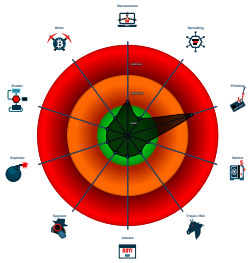

HTMLPhisher

| | |
|---|---|
| Score: | 48 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Yara detected HtmlPhish6
- HTML body contains low number of …
- HTML title does not match URL
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- None HTTPS page querying sensitiv…
- Suspicious form URL found

### Classification



## Startup

- **System is w10x64**
- iexplore.exe (PID: 5504 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1156 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5504 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

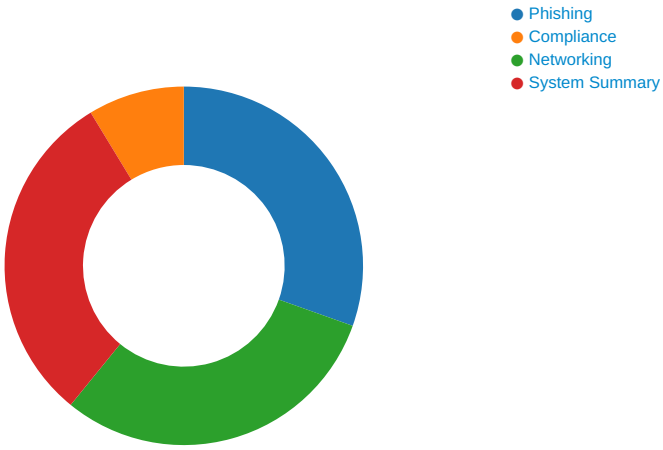
### Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| ensono8639844766FAXMESSAGE.HTM | JoeSecurity_HtmlPhish_6 | Yara detected HtmlPhish_6 | Joe Security | |

## Sigma Overview

**No Sigma rule has matched**

## Signature Overview




Click to jump to signature section

**Phishing:**

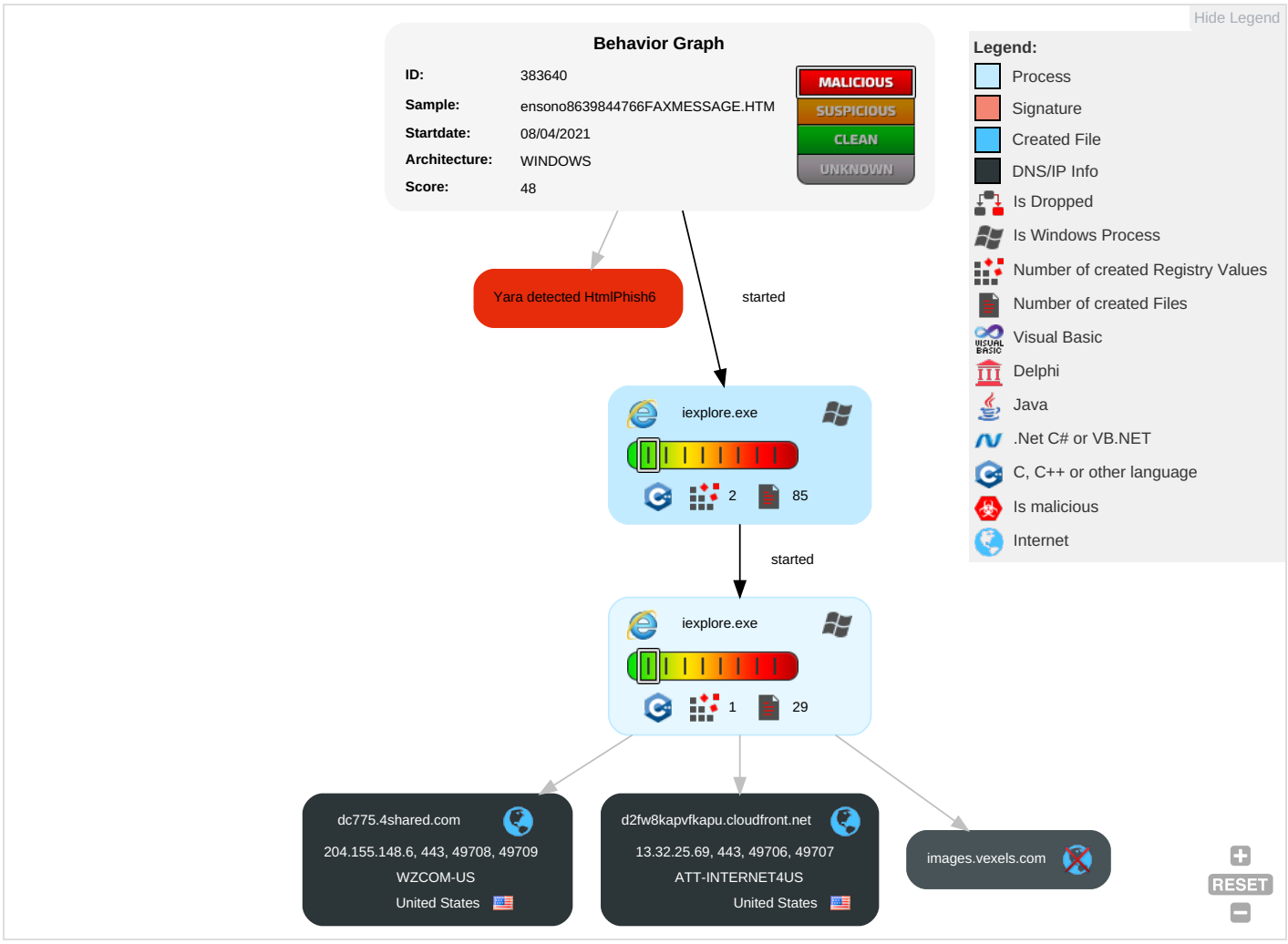


**Yara detected HtmlPhish6**

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impac |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation | Path Interception | Process Injection 1 | Masquerading 1 | OS Credential Dumping | File and Directory Discovery 1 | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Encrypted Channel 2 | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modif Syste Partiti |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Process Injection 1 | LSASS Memory | Application Window Discovery | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Non-Application Layer Protocol 1 | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Devic Lockc |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Obfuscated Files or Information 1 | Security Account Manager | Query Registry | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Application Layer Protocol 2 | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Delet Devic Data |

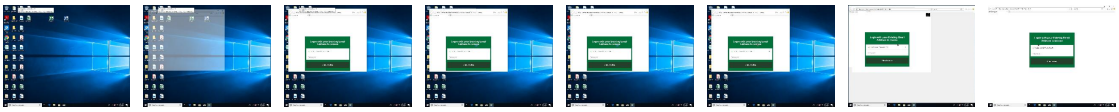
## Behavior Graph

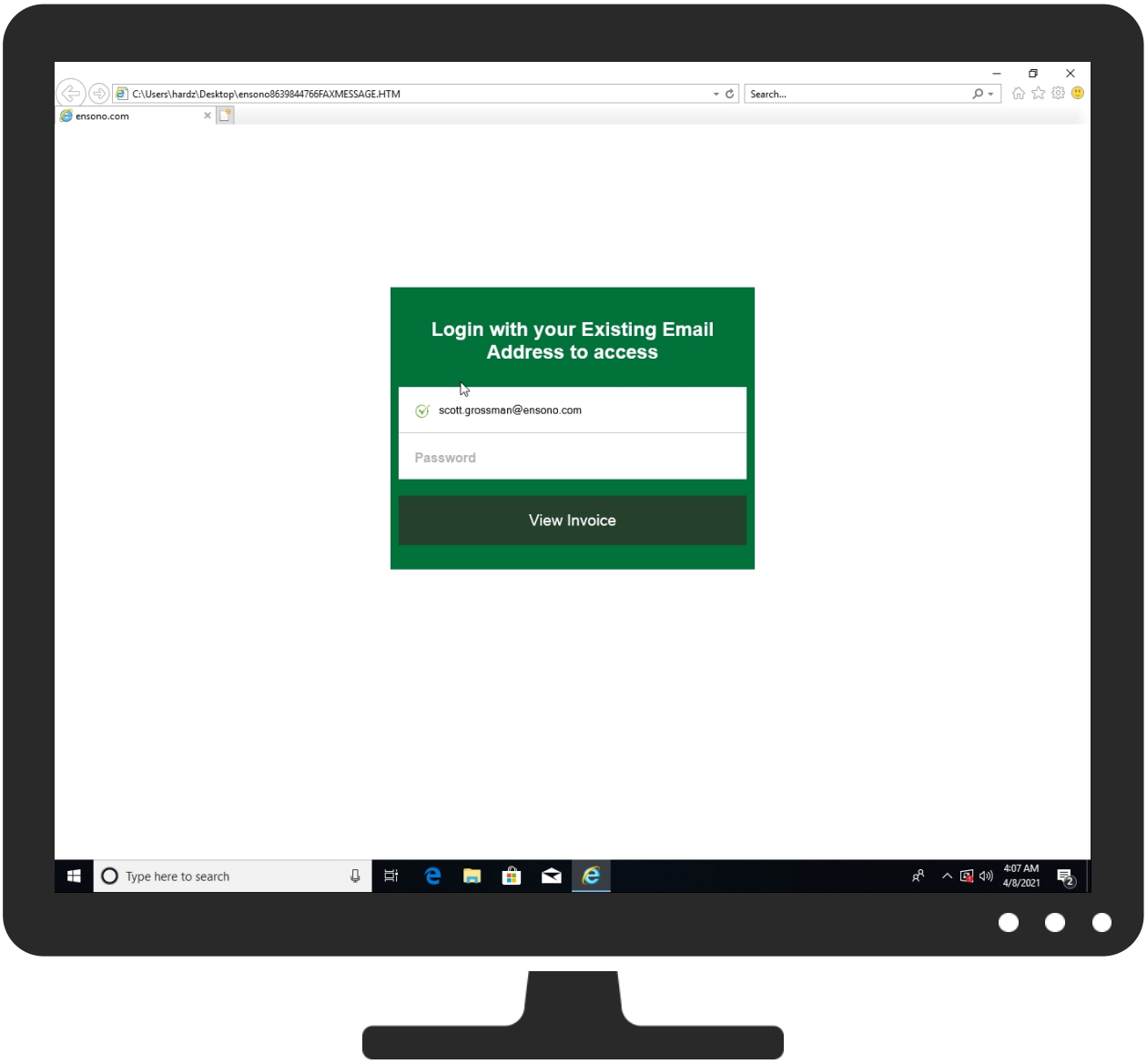



## Screenshots

### Thumbnails

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






## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

No Antivirus matches

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.wikipedia.com/ | 0% | URL Reputation | safe | |
| http://www.wikipedia.com/ | 0% | URL Reputation | safe | |
| http://www.wikipedia.com/ | 0% | URL Reputation | safe | |
| http://www.wikipedia.com/ | 0% | URL Reputation | safe | |

Copyright Joe Security LLC 2021

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| d2fw8kapvfkapu.cloudfront.net | 13.32.25.69 | true | false | | high |
| dc775.4shared.com | 204.155.148.6 | true | false | | high |
| images.vexels.com | unknown | unknown | false | | high |

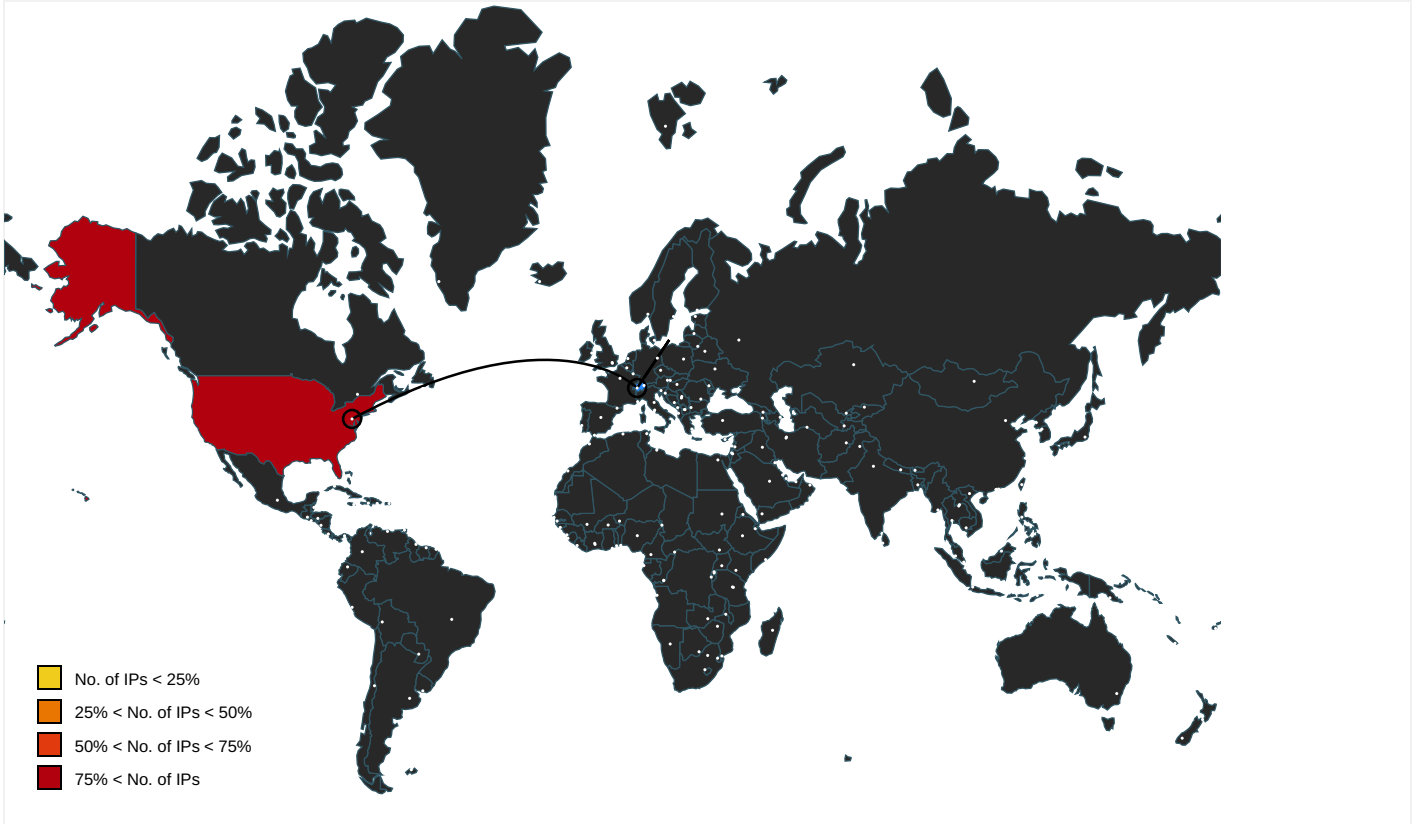
## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| file:///C:/Users/user/Desktop/ensono8639844766FAXMESSAGE.HTM | true | | low |

## URLs from Memory and Binaries

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://www.wikipedia.com/ | msapplication.xml6.1.dr | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://www.amazon.com/ | msapplication.xml.1.dr | false | | high |
| http://www.nytimes.com/ | msapplication.xml3.1.dr | false | | high |
| http://www.live.com/ | msapplication.xml2.1.dr | false | | high |
| http://www.reddit.com/ | msapplication.xml4.1.dr | false | | high |
| http://www.twitter.com/ | msapplication.xml5.1.dr | false | | high |
| http://www.youtube.com/ | msapplication.xml7.1.dr | false | | high |
| http://<br>https://dc775.4shared.com/img/5nLykkJeiq/s24/1749375d498/background?async&rand=0.707772242990717 | ensono8639844766FAXMESSAGE.HTM | false | | high |
| http://<br>https://images.vexels.com/media/users/3/157931/isolated/preview/604a0cadf94914c7ee6c6e552e9b4487-cur | ensono8639844766FAXMESSAGE.HTM | false | | high |

## Contacted IPs




## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 204.155.148.6 | dc775.4shared.com | United States | | 40824 | WZCOM-US | false |
| 13.32.25.69 | d2fw8kapvfkapu.cloudfront.net | United States | | 7018 | ATT-INTERNET4US | false |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 31.0.0 Emerald |
| Analysis ID: | 383640 |
| Start date: | 08.04.2021 |
| Start time: | 04:06:10 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 5m 7s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | ensono8639844766FAXMESSAGE.HTM |
| Cookbook file name: | defaultwindowshtmlcookbook.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: | 35 |
| 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: | mal48.phis.winHTM@3/16@2/2 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .HTM |

Copyright Joe Security LLC 2021

| Warnings: | Show All<br>• Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe<br>• TCP Packets have been reduced to 100<br>• Excluded IPs from analysis (whitelisted): 93.184.220.29, 40.88.32.150, 104.42.151.234, 168.61.161.212, 13.64.90.137, 104.83.120.32, 52.147.198.201, 20.82.210.154, 23.10.249.43, 23.10.249.26, 152.199.19.161, 23.54.113.104, 23.0.174.200, 23.0.174.185, 20.50.102.62, 20.54.26.129, 23.54.113.53, 52.155.217.156<br>• Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, go.microsoft.com, ocsp.digicert.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ie9comview.vo.msecnd.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, cs9.wpc.v0cdn.net |
|---|---|

# Simulations

## Behavior and APIs

**No simulations**

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 204.155.148.6 | UuEUqdfBXq.html | Get hash | malicious | Browse | |
| | FAX-MESSAGE6898352437.HTM | Get hash | malicious | Browse | |
| | FAX-MESSAGE6898352437.HTM | Get hash | malicious | Browse | |
| | FAX-MESSAGE6898352437.HTM | Get hash | malicious | Browse | |
| | Invoice-86383662834.HTML | Get hash | malicious | Browse | |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| dc775.4shared.com | UuEUqdfBXq.html | Get hash | malicious | Browse | • 204.155.148.6 |
| | FAX-MESSAGE6898352437.HTM | Get hash | malicious | Browse | • 204.155.148.6 |
| | FAX-MESSAGE6898352437.HTM | Get hash | malicious | Browse | • 204.155.148.6 |
| | FAX-MESSAGE6898352437.HTM | Get hash | malicious | Browse | • 204.155.148.6 |
| | Invoice-86383662834.HTML | Get hash | malicious | Browse | • 204.155.148.6 |
| d2fw8kapvfkapu.cloudfront.net | NEW PURCHASE ORDER.html | Get hash | malicious | Browse | • 13.226.162.81 |
| | Invoice-2334.HTML | Get hash | malicious | Browse | • 13.224.95.111 |
| | remittanceTT MT03.html | Get hash | malicious | Browse | • 13.224.95.111 |
| | INVOICE8637263.PDF.html | Get hash | malicious | Browse | • 13.224.95.79 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| WZCOM-US | N95lOmvdDI.exe | Get hash | malicious | Browse | • 208.94.232.134 |
| | WXqHhWniJN.exe | Get hash | malicious | Browse | • 208.94.232.134 |
| | 8tWIk1tWbK.exe | Get hash | malicious | Browse | • 208.94.232.134 |
| | kitten-weiss2020_com.dll | Get hash | malicious | Browse | • 185.186.245.185 |
| | Zadost o cenovou nabidku.doc | Get hash | malicious | Browse | • 204.155.149.140 |
| | Price Inquiry.doc | Get hash | malicious | Browse | • 199.101.134.238 |
| | vbConst.dll | Get hash | malicious | Browse | • 185.186.245.157 |
| | Transaccion de pago 31.03.2021.doc | Get hash | malicious | Browse | • 204.155.149.140 |
| | 000010052_02906666.doc | Get hash | malicious | Browse | • 199.101.134.238 |
| | PERuTR7vGb.dll | Get hash | malicious | Browse | • 185.186.247.42 |
| | 08uyd0CNTM.dll | Get hash | malicious | Browse | • 185.186.247.42 |
| | vbvlCb5GoP.dll | Get hash | malicious | Browse | • 185.186.247.42 |
| | Remittance_copy2021025678578485.HTM | Get hash | malicious | Browse | • 204.155.145.44 |
| | SecuriteInfo.com.W32.AIDetect.malware1.9324.exe | Get hash | malicious | Browse | • 185.186.245.62 |
| | FApiRVQ4a9.exe | Get hash | malicious | Browse | • 185.186.245.62 |
| | 602b97e0b415b.png.dll | Get hash | malicious | Browse | • 185.186.245.78 |
| | fvJmJ6fXtm.exe | Get hash | malicious | Browse | • 199.101.134.84 |
| | LDoSTuNuHc.rtf | Get hash | malicious | Browse | • 199.101.134.84 |
| | QRD289323_2020.docx | Get hash | malicious | Browse | • 199.101.134.84 |
| | http://tftpd32.jounin.net/tftpd32_download.html | Get hash | malicious | Browse | • 74.117.179.70 |
| ATT-INTERNET4US | Payment Report.html | Get hash | malicious | Browse | • 13.32.25.43 |
| | PaymentAdvice-copy.htm | Get hash | malicious | Browse | • 13.32.25.94 |
| | agmz0F8LbA.dll | Get hash | malicious | Browse | • 13.32.16.68 |
| | aunobp.dll | Get hash | malicious | Browse | • 13.32.16.68 |
| | document-1848152474.xlsm | Get hash | malicious | Browse | • 13.32.16.68 |
| | PDjf628Sns.exe | Get hash | malicious | Browse | • 69.232.46.139 |
| | 1637.xlsm | Get hash | malicious | Browse | • 13.32.16.68 |
| | 993.xlsm | Get hash | malicious | Browse | • 13.32.16.68 |
| | 2139.xlsm | Get hash | malicious | Browse | • 13.32.16.68 |
| | 3023.xlsm | Get hash | malicious | Browse | • 13.32.16.68 |
| | 2638.xlsm | Get hash | malicious | Browse | • 13.32.16.68 |
| | 3230.xlsm | Get hash | malicious | Browse | • 13.32.16.68 |
| | 2744.xlsm | Get hash | malicious | Browse | • 13.32.16.68 |
| | document-759334105.xls | Get hash | malicious | Browse | • 13.32.16.68 |
| | document-1784086484.xls | Get hash | malicious | Browse | • 13.32.16.68 |
| | document-1597268706.xls | Get hash | malicious | Browse | • 13.32.16.68 |
| | document-1315363159.xls | Get hash | malicious | Browse | • 13.32.16.68 |
| | document-1137036824.xls | Get hash | malicious | Browse | • 13.32.16.68 |
| | document-1981182525.xls | Get hash | malicious | Browse | • 13.32.16.68 |
| | document-170129283.xls | Get hash | malicious | Browse | • 13.32.16.68 |

## JA3 Fingerprints

Copyright Joe Security LLC 2021

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 9e10692f1b7f78228b2d4e424db3a98c | Payment Report.html | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | receipt-xxxx.htm | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | Mortgagor Request719350939.html | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | Receipt779G0D675432.html | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | PaymentAdvice-copy.htm | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | agmz0F8LbA.dll | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | vniSIKfm4h.dll | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | 61mwzdX4GC.dll | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | WbQrxxnmAO.dll | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | Invoice 880121.html | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | msals.pumpl.dll | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | Nickha #U0421#U0430ll Notification.mp3.htm | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | aunobp.dll | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | 606d810b8ff92.pdf.dll | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | syscshost.dll | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | syscshost.dll | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | DropDll.dll | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | lc.dll | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | FARASIS.xlsx | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |
| | msals.pumpl.dll | Get hash | malicious | Browse | • 204.155.148.6<br>• 13.32.25.69 |

## Dropped Files

**No context**

# Created / dropped Files

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{87E4B145-985A-11EB-90E4-ECF4BB862DED}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 30296 |
| Entropy (8bit): | 1.855028195520355 |
| Encrypted: | false |
| SSDEEP: | 96:rhZeZd2/WEQtEhfEkRbMEGJEnarEZfEVGLX:rhZeZd2/WhtofrNMX0yMfuMX |
| MD5: | 8DBA1019998701D6D49F18C044AB0932 |
| SHA1: | D43F144DA570AE2F13FC327E3492285CFD16E98E |
| SHA-256: | 2128EF68FF5AE8453A8531FEA0149730D2116C4CBF78C784BAAEAF4B12231F92 |
| SHA-512: | 44E6773FDBB139CBC5EF20D23DAD2AA88E40CE6E52ED5BA403EBDAF6AB3F51FFF5FBD6989C036457E8F7AD1DA73F24405ECD585DFDDA11F4464F17719C8E6BC2 |
| Malicious: | false |
| Reputation: | low |
| Preview: | .....<br>.....R.o.o.t. .E.n.t.r.<br>y.....<br>..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{87E4B147-985A-11EB-90E4-ECF4BB862DED}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 28506 |
| Entropy (8bit): | 1.9529654974532211 |
| Encrypted: | false |
| SSDEEP: | 96:rtZeQz6ZBSgjC2uWl/M4az7c47VFt6FWuUVuZuPonVEr:rtZeQz6ZkgjC2uWl/M4azY4BQVEr |
| MD5: | B5FC3D226F5CC2EC4B0D006B9DE707E1 |
| SHA1: | E35226BDE922D15DC594AA6DE97ACED34CB3EFA9 |
| SHA-256: | 182ADC59B8065B1851B6546FEAE779B81C5A0202F2FE992925B753F69F1940BF |
| SHA-512: | B36E31D431B265A89747BB7DF83D49FF5E57E9BB2AC981D21094469E2BBD8024D32AF7A99A4E62F72069357820D578A39A2912F637AACA52E8230DFFBAA791C |
| Malicious: | false |
| Reputation: | low |
| Preview: | .....R.o.o.t. .E.n.t.r.y..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{87E4B148-985A-11EB-90E4-ECF4BB862DED}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 16984 |
| Entropy (8bit): | 1.5655510714570202 |
| Encrypted: | false |
| SSDEEP: | 48:IwrGcprCGwpaPG4pQbGrapbSEGQpKCG7HpRsTGIpG:rxZqQB6PBScAtT4A |
| MD5: | E1E18421F6F0DE40E09176B263A297D2 |
| SHA1: | DC7F3B6787660188BA7CA569D434B88800F835B8 |
| SHA-256: | 4323293A6003CDB5183D1DE17F7B141153F9EA1C8A960B75838571C022FE332A |
| SHA-512: | DFE146AE1CE6FC31C8E271AF04D7B3CA0DFE26C32E282D1A0FEA7D691232D9783134FE80198450C7159C54A420A1F8C0FE8B4BFEC2F98D0C09A741C418F1DE<br>A |
| Malicious: | false |
| Reputation: | low |
| Preview: | .....R.o.o.t. .E.n.t.r.y..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 656 |
| Entropy (8bit): | 5.06821692286696 |
| Encrypted: | false |
| SSDEEP: | 12:TMHdNMNxOEWQ0gC9Q0g1nWimI002EtM3MHdNMNxOEWQ0gC9Q0g1nWimI00ObVbkt:2d6NxOhpj9p2SZHKd6NxOhpj9p2SZ76b |
| MD5: | E482F8C544825A10B3A46C4585803331 |
| SHA1: | 27A89733FCD8A0483EDCF0709E42119554042A95 |
| SHA-256: | 79EB17C0ECDDBCDDFE0326D0EFCA75BE97EACC57AF64831DD5C2E4CAEC05D9E6 |
| SHA-512: | 22A238CAAC4130E04EE343642E0B4BEABCDD5382EBF18087A388134564766E453061ABF8B23D1D28EF580CFA4F139255E7C75F5428A89A6E37321BD9A71FBA0 |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x5e0e732e,0x01d72c67</date><accdate>0x5e0e732e,0x01d72c67</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x5e0e732e,0x01d72c67</date><accdate>0x5e0e732e,0x01d72c67</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>.. |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 653 |
| Entropy (8bit): | 5.131753577358121 |
| Encrypted: | false |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml | |
|---|---|
| SSDEEP: | 12:TMHdNMNxe2kdM3iCgM3i1nWimI002EtM3MHdNMNxe2kdM3iCgM3i1nWimI00ObkS:2d6NxrrKSZHKd6NxrrKSZ7Aa7b |
| MD5: | 799C9F7BCB924571F13E07042362741E |
| SHA1: | 425A1742B0C0BC12E2F3D023964C67A78E88E120 |
| SHA-256: | 52C5C7A4700A4B0EB0B296229C78F42E775EA10AE5F2C972D381B59AFE4130C5 |
| SHA-512: | B69161A04CAB93D32EF2C304038D49AF8E6A453C0053EA6797512BE1C37747853D425A82EAEFC167CEDA3E15F2ED8772A9BC9BC76F2A0E0F00E64485F58C93C<br>A |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x5dfb604c,0x01d72c67</date><a<br>ccdate>0x5dfb604c,0x01d72c67</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?<br>xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x5dfb604c,0x01d72c67</date><a<br>ccdate>0x5dfb604c,0x01d72c67</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am<br>azon.url"/></tile></msapplication></browserconfig>.. |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 662 |
| Entropy (8bit): | 5.088458308724922 |
| Encrypted: | false |
| SSDEEP: | 12:TMHdNMNxvLWQ0gC9Q0g1nWimI002EtM3MHdNMNxvLWQ0gC9Q0g1nWimI00ObmZEs:2d6Nxvypj9p2SZHKd6Nxvypj9p2SZ7mb |
| MD5: | A58BC06697E0FAB5CEC9F032D27BC0B2 |
| SHA1: | D344A2ABFAAD80B2387069AB88398D080EE626F2 |
| SHA-256: | 34C4AECE8B45A14243E807100A30A534C59F010D708BF7062E720BBD890E80B0 |
| SHA-512: | 1384692EF8A9A0EE209945122BB30436A58AD2FAB23FC84549256E3603BA313691E46BA288EB0DF7522FB41DFFA638870CE54B6362BBC4B337073A29399DCCE6 |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x5e0e732e,0x01d72c67</date><br><accdate>0x5e0e732e,0x01d72c67</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?<br>xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x5e0e732e,0x01d72c67</date><accda<br>te>0x5e0e732e,0x01d72c67</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe<br>dia.url"/></tile></msapplication></browserconfig>.. |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 647 |
| Entropy (8bit): | 5.1277250897730395 |
| Encrypted: | false |
| SSDEEP: | 12:TMHdNMNxiYNCBN1nWimI002EtM3MHdNMNxiYNCBN1nWimI00Obd5EtMb:2d6NxjsBzSZHKd6NxjsBzSZ7Jjb |
| MD5: | 1739E2702E962F2718C01C38344D42B8 |
| SHA1: | 7EC6B10CC09DE1B48F67F7D1C6DE48BD7E96D0B8 |
| SHA-256: | 21CEB97722CA4B92FA21B168BE1A73490309715A4ABDC0D71E37D58DEBA5EEAF |
| SHA-512: | BD72092D4F82E5F4FEA8D42216453F1EC72F9832DB7528B014C694E4DE1D328195F18A5A56BF00FE806A57C25DAB76AEBF0F9D7A2608F752FA175518579D2686 |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x5e04e9b1,0x01d72c67</date><acc<br>date>0x5e04e9b1,0x01d72c67</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml<br>version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x5e04e9b1,0x01d72c67</date><accdate>0x5e04e<br>9b1,0x01d72c67</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile><br></msapplication></browserconfig>.. |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 656 |
| Entropy (8bit): | 5.102979409230783 |
| Encrypted: | false |
| SSDEEP: | 12:TMHdNMNxhGwWQ0gC9Q0g1nWimI002EtM3MHdNMNxhGwWQ0gC9Q0g1nWimI00Ob8V:2d6NxQ1pj9p2SZHKd6NxQ1pj9p2SZ7YV |
| MD5: | 5F99F62D93646032700BDEF24744E830 |
| SHA1: | 9BFCB729237483CAFE3E72F824BCD7159F6DE5B3 |
| SHA-256: | C338992F5C1563EF02ACD111ACD77B351A03233F93F6C28B7101C9E38786B1C2 |
| SHA-512: | 6FF536F890484F0A08F9ED4EC48B952226C7E9DB32B7235BF336240BA07017A2512715C1F66B66809C4EA7235CFEDE309E9119702D295FB7834F61577459BF4A |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml | |
|---|---|
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x5e0e732e,0x01d72c67</date><accdate>0x5e0e732e,0x01d72c67</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x5e0e732e,0x01d72c67</date><accdate>0x5e0e732e,0x01d72c67</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>.. |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 653 |
| Entropy (8bit): | 5.051385019709084 |
| Encrypted: | false |
| SSDEEP: | 12:TMHdNMNx0n2ACpA1nWimI002EtM3MHdNMNx0n2AC9Q0g1nWimI00ObxEtMb:2d6Nx0ElSZHKd6Nx0E9p2SZ7nb |
| MD5: | 766B75DC2A71858486A1F3CC9FB1E253 |
| SHA1: | B06786898356FF8A70CD45924FBB26ECA36023AB |
| SHA-256: | 97A8F26C422C3D0FEA7C0B381402CBA7EB95746AD3957C57E125ECE6BDA117FF |
| SHA-512: | A4A83AA1E4E586A9BC5D78F82A4585E9A5094CE52676FB08BFD711C8B2E45B48FFB428958328AF1F1E09DCDE33BA35B615C8659A5B5C3BBAC5EDE805422BF0D5 |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x5e0c10ee,0x01d72c67</date><accdate>0x5e0c10ee,0x01d72c67</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x5e0c10ee,0x01d72c67</date><accdate>0x5e0e732e,0x01d72c67</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>.. |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 656 |
| Entropy (8bit): | 5.0800162889446705 |
| Encrypted: | false |
| SSDEEP: | 12:TMHdNMNxx2ACpA1nWimI002EtM3MHdNMNxx2ACpA1nWimI00Ob6Kq5EtMb:2d6NxSISZHKd6NxSISZ7ob |
| MD5: | 26748B50766B3771BA30583EBF8975EF |
| SHA1: | B3E426E853D95C120A0BFF03EE0ACB50FBF94D71 |
| SHA-256: | 7B76115B6A34DF917D91A7E6311A18B5C3E3F6144D519CC62295B9B5E03D5C8A |
| SHA-512: | CC44F71426D7F894C467E8D8C45173DFFCABF885909AB30E1D7EF08F99B40C6638E6FF011711DD741B0EF40750E1C20B10D973282D97CB68C8D8D51D7C27AD |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x5e0c10ee,0x01d72c67</date><accdate>0x5e0c10ee,0x01d72c67</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x5e0c10ee,0x01d72c67</date><accdate>0x5e0c10ee,0x01d72c67</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>.. |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 659 |
| Entropy (8bit): | 5.099541863601186 |
| Encrypted: | false |
| SSDEEP: | 12:TMHdNMNxcM0CP01nWimI002EtM3MHdNMNxcM0CP01nWimI00ObVEtMb:2d6NxzCSZHKd6NxzCSZ7Db |
| MD5: | D49DA18192B16C8D3414026254288036 |
| SHA1: | AA777452EF8728C9D14DBEF37E7D9B853ECC1EB3 |
| SHA-256: | 4A1FB58860870791C0B41AACC1C7D530DC62F645FF572062C7C9D31C40FF6988 |
| SHA-512: | 84D28FC070328819E68F40E9262A96C8881B76F172C176266A557C9B82296C6BCB1BA5C254F8FC6C6BA2F755EC70DA632AB387711B7722116BEC2B5AD585CF3 |
| Malicious: | false |
| Reputation: | low |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml | |
|---|---|
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x5dfdc2a3,0x01d72c67</date><accdate>0x5dfdc2a3,0x01d72c67</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x5dfdc2a3,0x01d72c67</date><accdate>0x5dfdc2a3,0x01d72c67</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>.. |

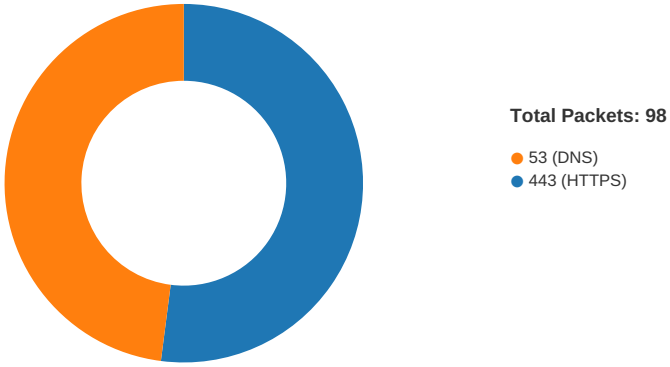
| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 653 |
| Entropy (8bit): | 5.113236116146009 |
| Encrypted: | false |
| SSDEEP: | 12:TMHdNMNxfnYNCBN1nWimI002EtM3MHdNMNxfnYNCBN1nWimI00Obe5EtMb:2d6NxQsBzSZHKd6NxQsBzSZ7ijb |
| MD5: | BB4CD44B0975D074B6FF8A5E727E2C56 |
| SHA1: | 1CC6D30077A207B3F6A13B1282C663CB7251BF27 |
| SHA-256: | 591FE7707F952636603D98A477D2A76B5C6DF81BB26A5BFFC827C126DDABD32E |
| SHA-512: | F86B4EFD097070647BA50732601B4FA2B544CCFCACB6C85122BFC8BD41675F2E8AB2E25B393F7049D1F9E096F4AA72D5C539217CEF26B30E9985431A6886F398 |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x5e04e9b1,0x01d72c67</date><accdate>0x5e04e9b1,0x01d72c67</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x5e04e9b1,0x01d72c67</date><accdate>0x5e04e9b1,0x01d72c67</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>.. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\604a0cadf94914c7ee6c6e552e9b4487-curved-check-mark-circle-icon-by-vexels[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 512 x 512, 16-bit/color RGBA, non-interlaced |
| Category: | downloaded |
| Size (bytes): | 153947 |
| Entropy (8bit): | 7.9846197450483 |
| Encrypted: | false |
| SSDEEP: | 3072:4czIFZWIctJrQzVBfCDngvAva1dDtd7JCnwqmvwCc7iF1qsaY65ZvUcAmlo:pEwTeB0a1dDtdKevwHiLfKvLS |
| MD5: | 64D70A176BB252ED0E41DB51B0229268 |
| SHA1: | 267E310F90705B1C9D607DAF0F2DA62AD6C09E80 |
| SHA-256: | 4CE3F26AC4C0D658CC3E3F51FADD97634AD178ADA224A97F8CA0B13C35791C2B |
| SHA-512: | 2549525EC51E6B6373A41077C28C7F9C5F697594D85998124B26D00371C7F9D89790D4887999399E8C6F4302FF8BBA58695FD3B32DF164656CD5991E89330D60 |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://images.vexels.com/media/users/3/157931/isolated/preview/604a0cadf94914c7ee6c6e552e9b4487-curved-check-mark-circle-icon-by-vexels.png |
| Preview: | .PNG.....IHDR.....gAMA.....a.....sRGB..... cHRM..z&.....u0...`.:....p..Q<....bKGD.....C.....pHYs...H...H.F.k>....IDATx...w.....[=3...%..IADr.A@D1"*bB..*H.J..L(*.....$A%...sX6.L...cfO....s.....;.;U.;.]-p..q..q..q

| C:\Users\user\AppData\Local\Temp\~DFACACD140C7DA886D.TMP | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 25441 |
| Entropy (8bit): | 1.2266349866132813 |
| Encrypted: | false |
| SSDEEP: | 96:kBqoxDhHWSVSE+ZO/m8LwojM0Jp5I8hYPhJzWPY2Sw3:kBqoxDhHjgE+C8ojM07JihCI |
| MD5: | 5D9A2D4EB539E1E1ED8DED2B1FFF97E2 |
| SHA1: | F57BFD990FD7F1D0CF9E75A613406A57E289C471 |
| SHA-256: | C8A645B31232CF54A108315E6E0541DF0C055105498E04BCC3AFCBBE77474F62 |
| SHA-512: | B3D623017F5FB801667A57AD9ED94A91F507492CE347D092E29B59093D496861DC07CDDEFC232BC4503564996BDC0497C3A90BB898BEF4B912F7A6C5C7E7660 |
| Malicious: | false |
| Reputation: | low |
| Preview: | .....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ..... ..... 

# Network Behavior

## Network Port Distribution




## TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Apr 8, 2021 04:06:59.222541094 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.222556114 CEST | 49706 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.240015984 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.240184069 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.240235090 CEST | 443 | 49706 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.240365028 CEST | 49706 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.245635033 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.246062040 CEST | 49706 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.262938976 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.263385057 CEST | 443 | 49706 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.263848066 CEST | 443 | 49706 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.263890028 CEST | 443 | 49706 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.263952971 CEST | 443 | 49706 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.263991117 CEST | 49706 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.264065981 CEST | 49706 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.265599966 CEST | 443 | 49706 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.265733004 CEST | 49706 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.266025066 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.266071081 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.266108036 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.266200066 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.266326904 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.269129038 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.269268036 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.308244944 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.308464050 CEST | 49706 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.313719034 CEST | 49708 | 443 | 192.168.2.3 | 204.155.148.6 |
| Apr 8, 2021 04:06:59.313848019 CEST | 49709 | 443 | 192.168.2.3 | 204.155.148.6 |
| Apr 8, 2021 04:06:59.316256046 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.316411972 CEST | 49706 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.316442966 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.325517893 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.325575113 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.325593948 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.325633049 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.325654984 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.325833082 CEST | 443 | 49706 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.326165915 CEST | 443 | 49706 | 13.32.25.69 | 192.168.2.3 |

Copyright Joe Security LLC 2021

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Apr 8, 2021 04:06:59.326199055 CEST | 443 | 49706 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.326240063 CEST | 49706 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.326270103 CEST | 49706 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.326445103 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.327307940 CEST | 49706 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.333609104 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.333666086 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.333704948 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.333826065 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.333913088 CEST | 443 | 49706 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.333956003 CEST | 443 | 49706 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.334029913 CEST | 49706 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.334856987 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.334882975 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.334918022 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.334923983 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.334948063 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.334974051 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.335289001 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.335314035 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.335336924 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.335349083 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.335376978 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.335969925 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.336031914 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.336051941 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.336091042 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.336105108 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.336149931 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.336755991 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.336816072 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.336838961 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.336877108 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.336910963 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.336987019 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.337491035 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.337553024 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.337572098 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.337616920 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.337671041 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.337734938 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.338449955 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.338510990 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.338535070 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.338593960 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.338610888 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.338674068 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.338838100 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.338882923 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.338891983 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.338916063 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.338952065 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.338989019 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.339693069 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.339731932 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.339776993 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.339792013 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.339837074 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.343543053 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.343596935 CEST | 443 | 49707 | 13.32.25.69 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.343621969 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |
| Apr 8, 2021 04:06:59.343647003 CEST | 49707 | 443 | 192.168.2.3 | 13.32.25.69 |

## UDP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Apr 8, 2021 04:06:49.914921045 CEST | 49199 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:06:49.927814960 CEST | 53 | 49199 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:06:50.745615005 CEST | 50620 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:06:50.758270025 CEST | 53 | 50620 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:06:51.373363972 CEST | 64938 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:06:51.385701895 CEST | 53 | 64938 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:06:52.292704105 CEST | 60152 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:06:52.305932999 CEST | 53 | 60152 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:06:53.025767088 CEST | 57544 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:06:53.038122892 CEST | 53 | 57544 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:06:53.752245903 CEST | 55984 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:06:53.765218973 CEST | 53 | 55984 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:06:54.740093946 CEST | 64185 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:06:54.752794027 CEST | 53 | 64185 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:06:56.586307049 CEST | 65110 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:06:56.600584030 CEST | 53 | 65110 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:06:57.684627056 CEST | 58361 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:06:57.698010921 CEST | 53 | 58361 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:06:57.783813000 CEST | 63492 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:06:57.805311918 CEST | 53 | 63492 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.055958033 CEST | 60831 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:06:59.068681002 CEST | 53 | 60831 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.166985035 CEST | 60100 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:06:59.182305098 CEST | 53195 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:06:59.198424101 CEST | 53 | 53195 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:06:59.310102940 CEST | 53 | 60100 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:01.273150921 CEST | 50141 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:01.285814047 CEST | 53 | 50141 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:02.571832895 CEST | 53023 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:02.583878040 CEST | 53 | 53023 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:14.737018108 CEST | 49563 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:14.751409054 CEST | 53 | 49563 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:15.836900949 CEST | 51352 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:15.849528074 CEST | 53 | 51352 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:16.804999113 CEST | 59349 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:16.817559958 CEST | 53 | 59349 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:17.993653059 CEST | 57084 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:18.006499052 CEST | 53 | 57084 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:19.756766081 CEST | 58823 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:19.770112991 CEST | 53 | 58823 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:21.166884899 CEST | 57568 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:21.179066896 CEST | 53 | 57568 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:21.856235027 CEST | 50540 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:21.868679047 CEST | 53 | 50540 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:24.990792990 CEST | 54366 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:25.009529114 CEST | 53 | 54366 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:27.758651018 CEST | 53034 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:27.771461964 CEST | 53 | 53034 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:28.049459934 CEST | 57762 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:28.073951006 CEST | 53 | 57762 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:28.474972963 CEST | 55435 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:28.489774942 CEST | 53 | 55435 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:29.111747980 CEST | 53034 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:29.125662088 CEST | 53 | 53034 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:29.486912966 CEST | 55435 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:29.500901937 CEST | 53 | 55435 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:30.746792078 CEST | 55435 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:30.751805067 CEST | 53034 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:30.759387016 CEST | 53 | 55435 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:30.764085054 CEST | 53 | 53034 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:32.751650095 CEST | 55435 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:32.752054930 CEST | 53034 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:32.765414953 CEST | 53 | 55435 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:32.765547991 CEST | 53 | 53034 | 8.8.8.8 | 192.168.2.3 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| Apr 8, 2021 04:07:36.767513037 CEST | 55435 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:36.767673016 CEST | 53034 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:36.780096054 CEST | 53 | 53034 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:36.780930042 CEST | 53 | 55435 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:45.050479889 CEST | 50713 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:45.068641901 CEST | 53 | 50713 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:07:57.019042969 CEST | 56132 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:07:57.030904055 CEST | 53 | 56132 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:08:01.484386921 CEST | 58987 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:08:01.502144098 CEST | 53 | 58987 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:08:33.376513004 CEST | 56579 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:08:33.389121056 CEST | 53 | 56579 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:08:41.668041945 CEST | 60633 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:08:41.681301117 CEST | 53 | 60633 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:08:44.012847900 CEST | 61292 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:08:44.030745029 CEST | 53 | 61292 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:09:27.414736032 CEST | 63619 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:09:27.427165985 CEST | 53 | 63619 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:09:27.795370102 CEST | 64938 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:09:27.821939945 CEST | 53 | 64938 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:09:42.448905945 CEST | 61946 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:09:42.516942978 CEST | 53 | 61946 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:09:42.847857952 CEST | 64910 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:09:42.908514023 CEST | 53 | 64910 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:09:43.290847063 CEST | 52123 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:09:43.305768967 CEST | 53 | 52123 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:09:43.816230059 CEST | 56130 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:09:43.829638004 CEST | 53 | 56130 | 8.8.8.8 | 192.168.2.3 |
| Apr 8, 2021 04:09:44.616730928 CEST | 56338 | 53 | 192.168.2.3 | 8.8.8.8 |
| Apr 8, 2021 04:09:44.708508968 CEST | 53 | 56338 | 8.8.8.8 | 192.168.2.3 |

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Apr 8, 2021 04:06:59.166985035 CEST | 192.168.2.3 | 8.8.8.8 | 0x22b | Standard query (0) | dc775.4shared.com | A (IP address) | IN (0x0001) |
| Apr 8, 2021 04:06:59.182305098 CEST | 192.168.2.3 | 8.8.8.8 | 0xebc8 | Standard query (0) | images.vexels.com | A (IP address) | IN (0x0001) |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Apr 8, 2021 04:06:59.198424101 CEST | 8.8.8.8 | 192.168.2.3 | 0xebc8 | No error (0) | images.vexels.com | d2fw8kapvfkapu.cloudfront.net | | CNAME (Canonical name) | IN (0x0001) |
| Apr 8, 2021 04:06:59.198424101 CEST | 8.8.8.8 | 192.168.2.3 | 0xebc8 | No error (0) | d2fw8kapvfkapu.cloudfront.net | | 13.32.25.69 | A (IP address) | IN (0x0001) |
| Apr 8, 2021 04:06:59.198424101 CEST | 8.8.8.8 | 192.168.2.3 | 0xebc8 | No error (0) | d2fw8kapvfkapu.cloudfront.net | | 13.32.25.96 | A (IP address) | IN (0x0001) |
| Apr 8, 2021 04:06:59.198424101 CEST | 8.8.8.8 | 192.168.2.3 | 0xebc8 | No error (0) | d2fw8kapvfkapu.cloudfront.net | | 13.32.25.34 | A (IP address) | IN (0x0001) |
| Apr 8, 2021 04:06:59.198424101 CEST | 8.8.8.8 | 192.168.2.3 | 0xebc8 | No error (0) | d2fw8kapvfkapu.cloudfront.net | | 13.32.25.101 | A (IP address) | IN (0x0001) |
| Apr 8, 2021 04:06:59.310102940 CEST | 8.8.8.8 | 192.168.2.3 | 0x22b | No error (0) | dc775.4shared.com | | 204.155.148.6 | A (IP address) | IN (0x0001) |

## HTTPS Packets

| Timestamp | Source IP | Source Port | Dest IP | Dest Port | Subject | Issuer | Not Before | Not After | JA3 SSL Client Fingerprint | JA3 SSL Client Digest |
|---|---|---|---|---|---|---|---|---|---|---|

| Timestamp | Source IP | Source Port | Dest IP | Dest Port | Subject | Issuer | Not Before | Not After | JA3 SSL Client Fingerprint | JA3 SSL Client Digest |
|---|---|---|---|---|---|---|---|---|---|---|
| Apr 8, 2021 04:06:59.265599966 CEST | 13.32.25.69 | 443 | 192.168.2.3 | 49706 | CN=images.vexels.com<br>CN=Amazon, OU=Server CA 1B, O=Amazon, C=US<br>CN=Amazon Root CA 1, O=Amazon, C=US<br>CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US | CN=Amazon, OU=Server CA 1B, O=Amazon, C=US<br>CN=Amazon Root CA 1, O=Amazon, C=US<br>CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US<br>OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US | Fri Oct 09 02:00:00 CEST 2020<br>Thu Oct 22 02:00:00 CEST 2015<br>Mon May 25 14:00:00 CEST 2015<br>Wed Sep 02 02:00:00 CEST 2009 | Tue Nov 09 13:00:00 CET 2021<br>Sun Oct 19 02:00:00 CEST 2025<br>Thu Dec 31 02:00:00 CET 2037<br>Wed Jun 28 19:39:16 CEST 2034 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
| | | | | | CN=Amazon, OU=Server CA 1B, O=Amazon, C=US | CN=Amazon Root CA 1, O=Amazon, C=US | Thu Oct 22 02:00:00 CEST 2015 | Sun Oct 19 02:00:00 CEST 2025 | | |
| | | | | | CN=Amazon Root CA 1, O=Amazon, C=US | CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US | Mon May 25 14:00:00 CEST 2015 | Thu Dec 31 02:00:00 CET 2037 | | |
| | | | | | CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US | OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US | Wed Sep 02 02:00:00 CEST 2009 | Wed Jun 28 19:39:16 CEST 2034 | | |
| Apr 8, 2021 04:06:59.269129038 CEST | 13.32.25.69 | 443 | 192.168.2.3 | 49707 | CN=images.vexels.com<br>CN=Amazon, OU=Server CA 1B, O=Amazon, C=US<br>CN=Amazon Root CA 1, O=Amazon, C=US<br>CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US | CN=Amazon, OU=Server CA 1B, O=Amazon, C=US<br>CN=Amazon Root CA 1, O=Amazon, C=US<br>CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US<br>OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US | Fri Oct 09 02:00:00 CEST 2020<br>Thu Oct 22 02:00:00 CEST 2015<br>Mon May 25 14:00:00 CEST 2015<br>Wed Sep 02 02:00:00 CEST 2009 | Tue Nov 09 13:00:00 CET 2021<br>Sun Oct 19 02:00:00 CEST 2025<br>Thu Dec 31 02:00:00 CET 2037<br>Wed Jun 28 19:39:16 CEST 2034 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
| | | | | | CN=Amazon, OU=Server CA 1B, O=Amazon, C=US | CN=Amazon Root CA 1, O=Amazon, C=US | Thu Oct 22 02:00:00 CEST 2015 | Sun Oct 19 02:00:00 CEST 2025 | | |
| | | | | | CN=Amazon Root CA 1, O=Amazon, C=US | CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US | Mon May 25 14:00:00 CEST 2015 | Thu Dec 31 02:00:00 CET 2037 | | |
| | | | | | CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US | OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US | Wed Sep 02 02:00:00 CEST 2009 | Wed Jun 28 19:39:16 CEST 2034 | | |

| Timestamp | Source IP | Source Port | Dest IP | Dest Port | Subject | Issuer | Not Before | Not After | JA3 SSL Client Fingerprint | JA3 SSL Client Digest |
|---|---|---|---|---|---|---|---|---|---|---|
| Apr 8, 2021 04:06:59.594474077 CEST | 204.155.148.6 | 443 | 192.168.2.3 | 49709 | CN=*.4shared.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US | CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US | Mon Jun 29 00:54:17 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004 | Wed Jun 29 00:54:17 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
| | | | | | CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US | CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US | Tue May 03 09:00:00 CEST 2011 | Sat May 03 09:00:00 CEST 2031 | | |
| | | | | | CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US | OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US | Wed Jan 01 08:00:00 CET 2014 | Fri May 30 09:00:00 CEST 2031 | | |
| | | | | | OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US | OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US | Tue Jun 29 19:06:20 CEST 2004 | Thu Jun 29 19:06:20 CEST 2034 | | |
| Apr 8, 2021 04:06:59.595632076 CEST | 204.155.148.6 | 443 | 192.168.2.3 | 49708 | CN=*.4shared.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US | CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US | Mon Jun 29 00:54:17 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004 | Wed Jun 29 00:54:17 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0 | 9e10692f1b7f78228b2d4e424db3a98c |
| | | | | | CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US | CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US | Tue May 03 09:00:00 CEST 2011 | Sat May 03 09:00:00 CEST 2031 | | |
| | | | | | CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US | OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US | Wed Jan 01 08:00:00 CET 2014 | Fri May 30 09:00:00 CEST 2031 | | |
| | | | | | OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US | OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US | Tue Jun 29 19:06:20 CEST 2004 | Thu Jun 29 19:06:20 CEST 2034 | | |

## Code Manipulations

# Statistics

## Behavior




Click to jump to process

# System Behavior

## Analysis Process: iexplore.exe PID: 5504 Parent PID: 792

### General

| | |
|---|---|
| Start time: | 04:06:56 |
| Start date: | 08/04/2021 |
| Path: | C:\Program Files\internet explorer\iexplore.exe |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding |
| Imagebase: | 0x7ff6ef370000 |
| File size: | 823560 bytes |
| MD5 hash: | 6465CB92B25A7BC1DF8E01D8AC5E7596 |
| 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 |
|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

### Registry Activities

| Key Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| Key Path | Name | Type | Old Data | New Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

Copyright Joe Security LLC 2021

## Analysis Process: iexplore.exe PID: 1156 Parent PID: 5504

### General

| | |
|---|---|
| Start time: | 04:06:57 |
| Start date: | 08/04/2021 |
| Path: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5504 CREDAT:17410 /prefetch:2 |
| Imagebase: | 0xaa0000 |
| File size: | 822536 bytes |
| MD5 hash: | 071277CC2E3DF41EEEA8013E2AB58D5A |
| 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 |
|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

### Registry Activities

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

## Disassembly