


**ID:** 412528
**Cookbook:** browseurl.jbs
**Time:** 18:51:41
**Date:** 12/05/2021
**Version:** 32.0.0 Black Diamond

# Table of Contents

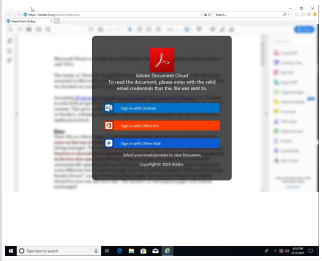
# Analysis Report https://landarch.org/hassani/index.php

## Overview

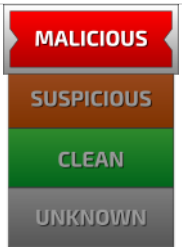
### General Information

| | |
|---|---|
| Sample URL: | http://https://landarch.org/hassani/index.php |
| Analysis ID: | 412528 |
| Infos: | |

Most interesting Screenshot:



### Detection



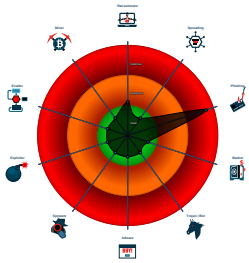

HTMLPhisher

| | |
|---|---|
| Score: | 76 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Antivirus / Scanner detection for sub…
- Phishing site detected (based on sh…
- Yara detected HtmlPhish10
- Yara detected HtmlPhish7
- Phishing site detected (based on va…
- HTML body contains low number of …
- HTML title does not match URL

### Classification



## Startup

- **System is w10x64**
- iexplore.exe (PID: 1972 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5784 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1972 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

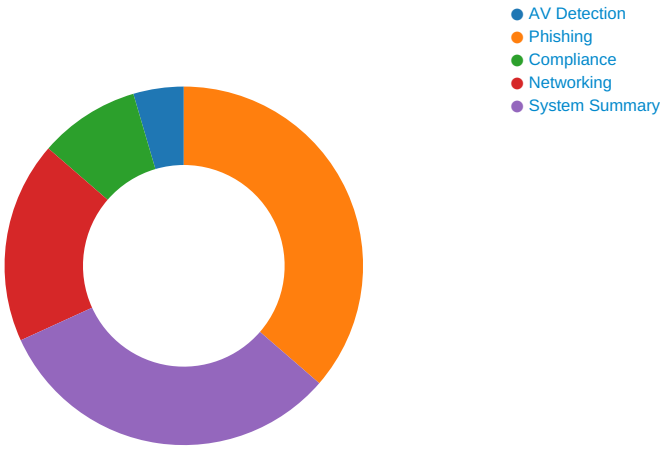
### Dropped Files

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\index[1].htm | JoeSecurity_HtmlPhish_10 | Yara detected HtmlPhish_10 | Joe Security | |
| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\index[1].htm | JoeSecurity_HtmlPhish_7 | Yara detected HtmlPhish_7 | Joe Security | |

## Sigma Overview

**No Sigma rule has matched**

## Signature Overview




Click to jump to signature section

## AV Detection:

**Antivirus / Scanner detection for submitted sample**

## Phishing:

**Phishing site detected (based on shot template match)**

**Yara detected HtmlPhish10**

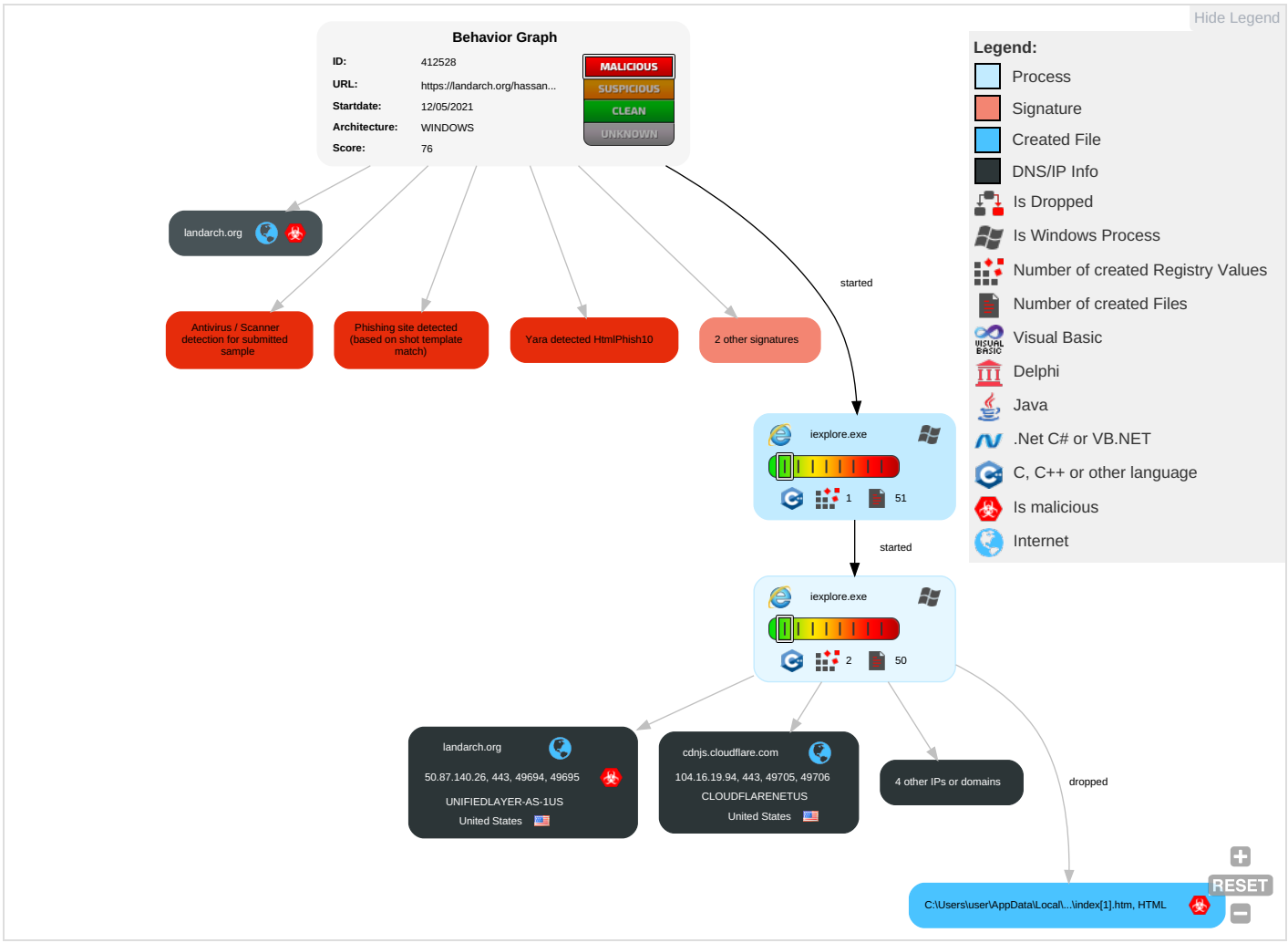
**Yara detected HtmlPhish7**

**Phishing site detected (based on various OCR indicators)**

## 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 | 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 |

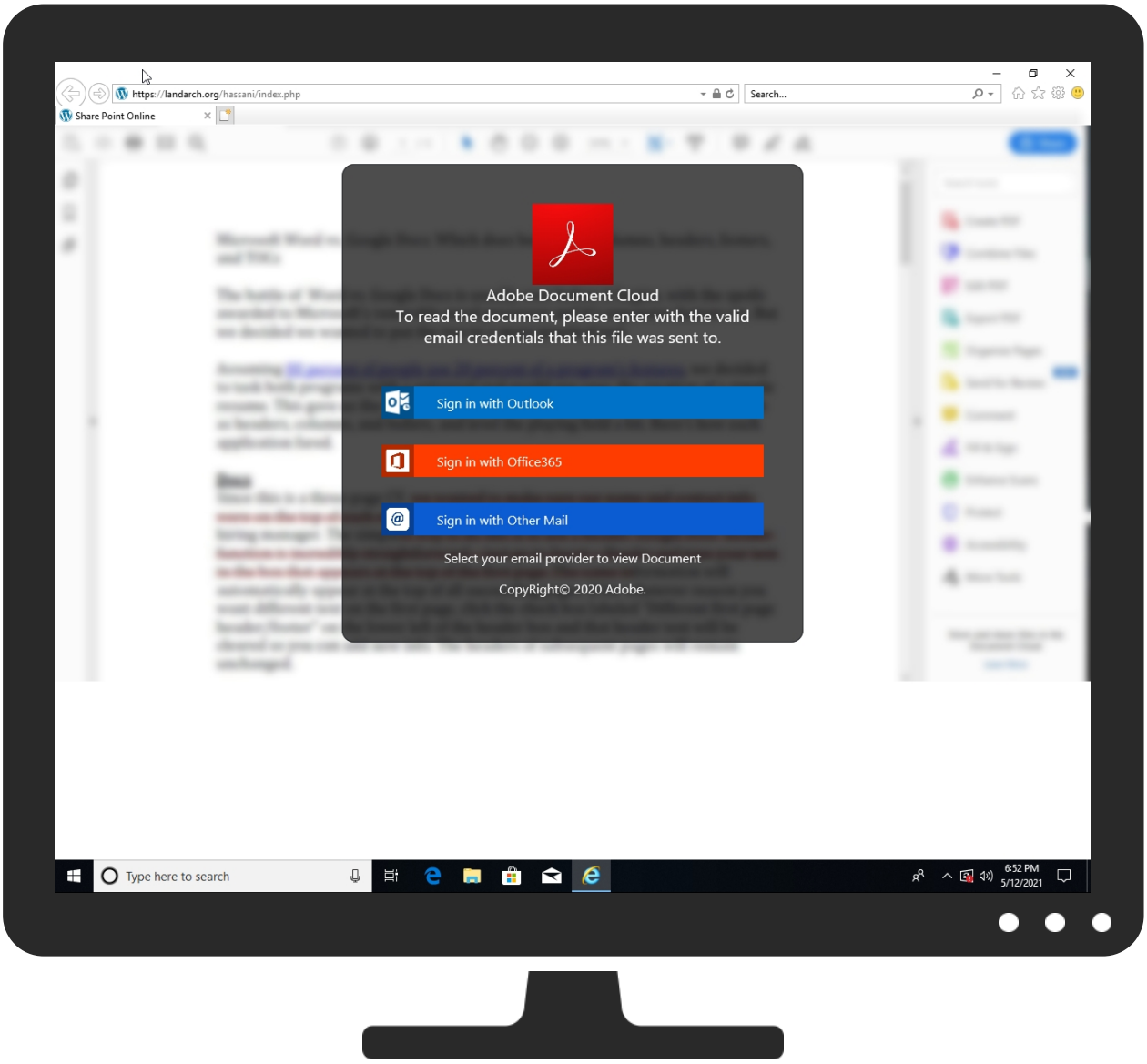
## Behavior Graph




## 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

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://landarch.org/hassani/index.php | 0% | Avira URL Cloud | safe | |
| http://https://landarch.org/hassani/index.php | 100% | SlashNext | Fake Login Page type: Phishing & Social usering | |

## Dropped Files

No Antivirus matches

## Unpacked PE Files

No Antivirus matches

## Domains

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| landarch.org | 0% | Virustotal | | Browse |

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://ianlunn.github.io/Hover/) | 0% | Virustotal | | Browse |
| http://ianlunn.github.io/Hover/) | 0% | Avira URL Cloud | safe | |
| http://https://landarch.org/favicon.ico | 0% | Avira URL Cloud | safe | |
| http://https://landarch.org/hassani/index.php$Share | 0% | Avira URL Cloud | safe | |
| http://https://landarch.org/hassani/index.phpRoot | 0% | Avira URL Cloud | safe | |
| http://https://getbootstrap.com) | 0% | Avira URL Cloud | safe | |
| http://ianlunn.co.uk/ | 0% | URL Reputation | safe | |
| http://ianlunn.co.uk/ | 0% | URL Reputation | safe | |
| http://ianlunn.co.uk/ | 0% | URL Reputation | safe | |
| http://https://landarch.org/hassani/index.phpn | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| cdnjs.cloudflare.com | 104.16.19.94 | true | false | | high |
| maxcdn.bootstrapcdn.com | 104.18.10.207 | true | false | | high |
| landarch.org | 50.87.140.26 | true | true | • 0%, Virustotal, Browse | unknown |
| ka-f.fontawesome.com | unknown | unknown | false | | high |
| code.jquery.com | unknown | unknown | false | | high |
| kit.fontawesome.com | unknown | unknown | false | | high |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://landarch.org/hassani/index.php | true | | unknown |

## URLs from Memory and Binaries

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://ianlunn.github.io/Hover/) | hover[1].css.2.dr | false | • 0%, Virustotal, Browse<br>• Avira URL Cloud: safe | unknown |
| http://https://ka-f.fontawesome.com | 585b051251[1].js.2.dr | false | | high |
| http://https://code.jquery.com/jquery-3.2.1.slim.min.js | index[1].htm.2.dr | false | | high |
| http://https://landarch.org/favicon.ico | imagestore.dat.2.dr | false | • Avira URL Cloud: safe | unknown |
| http://https://code.jquery.com/jquery-3.1.1.min.js | index[1].htm.2.dr | false | | high |
| http://https://landarch.org/hassani/index.php$Share | {E0B0444A-B38D-11EB-90E5-ECF4BB2D2496}.dat.1.dr | true | • Avira URL Cloud: safe | unknown |
| http://https://code.jquery.com/jquery-3.3.1.js | index[1].htm.2.dr | false | | high |
| http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css | index[1].htm.2.dr | false | | high |
| http://https://fontawesome.com/license/free | free.min[1].css.2.dr | false | | high |
| http://https://landarch.org/hassani/index.phpRoot | {E0B0444A-B38D-11EB-90E5-ECF4BB2D2496}.dat.1.dr | true | • Avira URL Cloud: safe | unknown |
| http://https://fontawesome.com | free.min[1].css.2.dr | false | | high |
| http://https://kit.fontawesome.com | 585b051251[1].js.2.dr | false | | high |
| http://https://github.com/twbs/bootstrap/graphs/contributors) | bootstrap.min[1].js.2.dr | false | | high |
| http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js | index[1].htm.2.dr | false | | high |
| http://https://login.microsoftonline.com/common/login | index[1].htm.2.dr | false | | high |
| http://https://getbootstrap.com) | bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr | false | • Avira URL Cloud: safe | low |
| http://ianlunn.co.uk/ | hover[1].css.2.dr | false | • URL Reputation: safe<br>• URL Reputation: safe<br>• URL Reputation: safe | unknown |
| http://https://github.com/twbs/bootstrap/blob/master/LICENSE) | bootstrap.min[1].js.2.dr, bootstrap.min[1].css.2.dr | false | | high |
| http://https://github.com/IanLunn/Hover | hover[1].css.2.dr | false | | high |
| http://https://landarch.org/hassani/index.php | {E0B0444A-B38D-11EB-90E5-ECF4BB2D2496}.dat.1.dr | true | | unknown |
| http://opensource.org/licenses/MIT). | popper.min[1].js.2.dr | false | | high |
| http://https://kit.fontawesome.com/585b051251.js | index[1].htm.2.dr | false | | high |

| Name | Source | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|
| http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js | index[1].htm.2.dr | false | | high |
| http://https://landarch.org/hassani/index.phpn | {E0B0444A-B38D-11EB-90E5-ECF4BB2D2496}.dat.1.dr | true | • Avira URL Cloud: safe | unknown |

## Contacted IPs


## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 50.87.140.26 | landarch.org | United States | | 46606 | UNIFIEDLAYER-AS-1US | true |
| 104.18.10.207 | maxcdn.bootstrapcdn.com | United States | | 13335 | CLOUDFLARENETUS | false |
| 104.16.19.94 | cdnjs.cloudflare.com | United States | | 13335 | CLOUDFLARENETUS | false |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 32.0.0 Black Diamond |
| Analysis ID: | 412528 |
| Start date: | 12.05.2021 |
| Start time: | 18:51:41 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 2m 56s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Cookbook file name: | browseurl.jbs |
| Sample URL: | http://https://landarch.org/hassani/index.php |
| 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: | 3 |
| 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: | • EGA enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal76.phis.win@3/26@7/3 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI |
| Warnings: | Show All<br>• Excluded IPs from analysis (whitelisted): 52.147.198.201, 13.88.21.125, 88.221.62.148, 104.43.139.144, 142.250.185.234, 69.16.175.10, 69.16.175.42, 142.250.184.234, 104.18.22.52, 104.18.23.52, 172.64.101.17, 172.64.100.17<br>• TCP Packets have been reduced to 100<br>• Excluded domains from analysis (whitelisted): kit.fontawesome.com.cdn.cloudflare.net, cds.s5x3j6q5.hwcdn.net, fonts.googleapis.com, ka-f.fontawesome.com.cdn.cloudflare.net, ajax.googleapis.com, skypedataprdcolcus16.cloudapp.net, skypedataprdcoleus16.cloudapp.net, e11290.dspg.akamaiedge.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, watson.telemetry.microsoft.com, skypedataprdcolwus15.cloudapp.net<br>• Report size getting too big, too many NtDeviceIoControlFile calls found. |

# Simulations

## Behavior and APIs

**No simulations**

# Joe Sandbox View / Context

## IPs

**No context**

## Domains

**No context**

## ASN

**No context**

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{E0B04448-B38D-11EB-90E5-ECF4BB2D2496}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 30296 |
| Entropy (8bit): | 1.8529727739977848 |
| Encrypted: | false |
| SSDEEP: | 96:r4ZrZF2oWUtFAfYHT1MCrT3RRC+fZHulX:r4ZrZF2oWUtOfYBMEznfZsX |
| MD5: | 6E807F25A7992663FDA5A565C66C679A |
| SHA1: | E1B68DACD3684EE530E150BAAC538DF2A2F203B5 |
| SHA-256: | 399B5ED01496B5BC8B31E4D765A26D100DD84B348EDC68DA931A7175C8076842 |
| SHA-512: | 68AF0AA6E1649150E62D29463C53FF09966EF2952FA330B1E31C8FF46D8351A134CB20860E02B5CB2EDF329FB3521B796CF60355698D97574B1B4C1CA45758F0 |
| 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\{E0B0444A-B38D-11EB-90E5-ECF4BB2D2496}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 27424 |
| Entropy (8bit): | 1.7717716723673704 |
| Encrypted: | false |
| SSDEEP: | 48:Iw01GcpryGwpayG4pQaGrapbSbGQpByGHHpc8TGUp8jGzYpm7DGopKRhxoGOXpRU:r6Z6QC6MBSVjJ20W5MJAByTwsbwr |
| MD5: | 3D364410D65A99450FC4C2EF4321680F |
| SHA1: | C2AFAD48A380C38C021D4C8871F2CAE60A99BBD6 |
| SHA-256: | 87B27269631CCD2C7C393E5C8A9911512D595856BB63E1E563E036C9CA918E87 |
| SHA-512: | 655529D59612675AB7DCF37877F37DC8CB1BE63DCA2AABB081C6C3F120EA8B769A853E803D9CFFA75C92BFDA86C2A6743506D2293CDFA7E7B7261257B61AC9EE |
| 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\{E7627DA5-B38D-11EB-90E5-ECF4BB2D2496}.dat | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | Microsoft Word Document |
| Category: | dropped |
| Size (bytes): | 16984 |
| Entropy (8bit): | 1.5654132269703587 |
| Encrypted: | false |
| SSDEEP: | 48:IwdEGcprTvGwpaVEG4pQH2GrapbS5GQpKSG7HpRFTGIpG:rWZ1QK6YBSTA9TTA |
| MD5: | FE97198667617515C0C2B70744B7E782 |
| SHA1: | A7E45A67E9D77451F295115A1DAC2C398BE82F3B |
| SHA-256: | 701D6DC4A9FD3F6484CA00324FF630F7CDC5D591C635A1D33074595DE4887D97 |
| SHA-512: | F938A29EE77AB2DB2954D3424DC4A96F219AEB47E0185666F078C15CEF6245C773317F461DC27105047716BB45EEFBC5C8BE3F7F88C2CA5B86DECF93219AE52 |
| Malicious: | false |
| Reputation: | low |
| Preview: | .....R.o.o.t. .E.n.t.r.y..... |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | data |
| Category: | modified |
| Size (bytes): | 4221 |
| Entropy (8bit): | 7.9241968052279805 |
| Encrypted: | false |
| SSDEEP: | 96:y3bdWfcmTY+aRF1pXWZL2+42HGhIUc8KeLEy:ygXTY+as02mOB8XLEy |

| C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat | |
|---|---|
| MD5: | F33B4E5589E4FFF7F2FBFB1D72DEF0CF |
| SHA1: | A55535DCBD9B6624E73889399B52DE1841FDDE48 |
| SHA-256: | 31ED31DD86D7E6A27C714CD23F5E188E0D33657BA295F57DD8954F61283D06B2 |
| SHA-512: | 0571E2B0D8D670045C19E1CB1CB5A47D3E391159867D9329CE5F9FA5CEC787B7201F82A575B0C1C8ACD0E9424A519B38500A9D41E5C814E78F794FC3A2C9CB<br>B |
| Malicious: | false |
| Reputation: | low |
| Preview: | .h.t.t.p.s.:././.l.a.n.d.a.r.c.h...o.r.g./.f.a.v.i.c.o.n...i.c.o.....PNG.....IHDR...P...P.....IDATx..].xU...[..V..*).Kk...V.k..J]jKEl?...t...!.{.,...E.....@....F.%.....B...N.y..w.....l{.o...;.s..<br>3...WH...../.zBp.o,XW.....#Z.f...\|mvD..9..F.....y..o....1^.743l.....v..#.c.E&.e..hU1.{....._cZ..We.v.....f.w....(..6\|.Y.. I:x..-.&.....D.....<.6.6.l....T..)...\|....#..$g...VN.....<br>.!'/6.w..B.h.}....EV.....k.7" f.}.G.~#..M..+....G....iB.....]..?+.....'.j.GB..P%.....\...../..%...&.8E..".....44.J...1.....S.....d.j..]ni%._..9.{.O?.H..6T.\|A.GC..g...U.oDEt,?.<br>0....~....q=.y.~.9.Z.....c...v..\_....$.0.2...F.9a.L..)..I...2...w...I..&....Vg.....H.I..r...../....z.`..+...Z.^U.=..5aBpb..0< ../>.9.c....".I..0.3N,}}....]Fb...Q.....W.....OQ..y;.....\|.37..}.....<br>(c.....X..`xX).;.....<5S....>.9..G.:...=..0^.....I_<G.....H....C.O.*.....Hk{..{....]Nc..B.8..}%>..w....Z...).....\..>....c..2...&..0' |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\adobe[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | JPEG image data, JFIF standard 1.02, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 400x400, frames 3 |
| Category: | downloaded |
| Size (bytes): | 30925 |
| Entropy (8bit): | 7.75667128400845 |
| Encrypted: | false |
| SSDEEP: | 768:nuowBuvTpjgz+wqrPZ2qh8fmyjlX6RqnxgYqwNL:nuPOpjgzPqrPZRYZGnYqYL |
| MD5: | BE5274AF7D8BD25B8148A190FF515399 |
| SHA1: | B8D0850FD92EE935287E17988B89E53607808C8C |
| SHA-256: | 26C62DBDF527B8DCBF378EA62F129CBBBA3B244730687909BA21ECD729C9D2E6 |
| SHA-512: | 64893C625BE72783088575E36EF26FF4573243F32601BDA754EDA72B7515063B5E4E4831697D16AC663529C910AE12CCD145BEC530F2A9BAE4D9324301C65667 |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://landarch.org/hassani/images/adobe.jpg |
| Preview: | .....JFIF.....C.....C.....".....}.....!1A..Qa."q.<br>2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ<br>.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..g.....\|?....".+....._.....4...R...'..q..<br>~...n.7.....QXJ<...=...^.V'@U..E..5....Uz.....IE.PTe.}/p.y.....T.<...-T..\|...b.=.#IU..~....{O/...b..E.....X...G...?.....\|....._....M..g.....T~g.....<.....T~g.....3$.=._..<br>IU.K..^.E...=.#U.._[X.R..=W...1.....QTr.\....*.7..?..6.9K..^.E.Ps.\.....%W..y...g)s[KX)<..... |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\free-v4-shims.min[1].css | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with very long lines |
| Category: | downloaded |
| Size (bytes): | 26701 |
| Entropy (8bit): | 4.829823522211244 |
| Encrypted: | false |
| SSDEEP: | 192:dP6hT1bIl4w0QUmQ10PwKLaAu5CwWavpHo4O6wgLPbJVR8XD7mycP:0hal4w0QK+PwK05eavpmgPPeXD7mycP |
| MD5: | 8A99CE81EC2F89FBCA03F2C8CF1A3679 |
| SHA1: | 58F9EF32D12A5DA52CBAB7BD518BCC998FC59EF9 |
| SHA-256: | 362DAEAF1F7E05FEE9A609E549F148AACBE518C166FBD96EAD69057E295742AF |
| SHA-512: | 930F28449365FAED13718BB8F332625DB110ABB08C3778DC632FDF00A0187A61A086B5EB4765FFC1923B64E2584C02592A213914B024DE6890FF3DBFC3A12FE5 |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://ka-f.fontawesome.com/releases/v5.15.3/css/free-v4-shims.min.css?token=585b051251 |
| Preview: | /*!. * Font Awesome Free 5.15.3 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa.fa-glass:before{content:"\f000"}.fa.fa-meetup{font-family:"Font Awesome 5 Brands";font-weight:400}.fa.fa-star-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-star-o:before{content:"\f005"}.fa.fa-close:before,.fa.fa-remove:before{content:"\f00d"}.fa.fa-gear:before{content:"\f013"}.fa.fa-trash-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-trash-o:before{content:"\f2ed"}.fa.fa-file-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-file-o:before{content:"\f15b"}.fa.fa-clock-o{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-clock-o:before{content:"\f017"}.fa.fa-arrow-circle-o-down{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arrow-circle-o-down:before{content:"\f358"}.fa.fa-arrow-circle-o-up{font-family:"Font Awesome 5 Free";font-weight:400}.fa.fa-arro |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\free.min[1].css | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with very long lines |
| Category: | downloaded |
| Size (bytes): | 60351 |
| Entropy (8bit): | 4.728641238865369 |
| Encrypted: | false |
| SSDEEP: | 768:0Uh31IPiyXNq4YxBowbgJlkwF//zMQyYJYX9Bft6VSz8:0U0PxXE4YXJgndFTfy9lt5Q |
| MD5: | 390B4210E10C744C3C597500BCF0B31A |
| SHA1: | 2600C7C2F25D7DBCBC668231601E426010DC6489 |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\free.min[1].css | |
|---|---|
| SHA-256: | C2819CA1F7AD1AF7BA53C4EDFDFD395C547BCB16D29892A234D7860C689ED929 |
| SHA-512: | E8A7E466BE8CC092E12994B51A6A8A39E2FBB66DD48221BCF499BB89365B4004D73C1909F8FE0BBBBF13907D5901D76FFE127D92FDD7493853646F83F5985CB |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://ka-f.fontawesome.com/releases/v5.15.3/css/free.min.css?token=585b051251 |
| Preview: | /*!. * Font Awesome Free 5.15.3 by @fontawesome - https://fontawesome.com. * License - https://fontawesome.com/license/free (Icons: CC BY 4.0, Fonts: SIL OFL 1.1, Code: MIT License). */.fa,.fab,.fad,.fal,.far,.fas{-moz-osx-font-smoothing:grayscale;-webkit-font-smoothing:antialiased;display:inline-block;font-style:normal;font-variant:normal;text-rendering:auto;line-height:1}.fa-lg{font-size:1.33333em;line-height:.75em;vertical-align:-.0667em}.fa-xs{font-size:.75em}.fa-sm{font-size:.875em}.fa-1x{font-size:1em}.fa-2x{font-size:2em}.fa-3x{font-size:3em}.fa-4x{font-size:4em}.fa-5x{font-size:5em}.fa-6x{font-size:6em}.fa-7x{font-size:7em}.fa-8x{font-size:8em}.fa-9x{font-size:9em}.fa-10x{font-size:10em}.fa-fw{text-align:center;width:1.25em}.fa-ul{list-style-type:none;margin-left:2.5em;padding-left:0}.fa-ul>li{position:relative}.fa-li{left:-2em;position:absolute;text-align:center;width:2em;line-height:inherit}.fa-border{border:.08em solid #eee;border-radius:.1em;padding:.2em .25em .15em}.fa-pul |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\jquery.min[1].js | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with very long lines |
| Category: | downloaded |
| Size (bytes): | 85578 |
| Entropy (8bit): | 5.366055229017455 |
| Encrypted: | false |
| SSDEEP: | 1536:EYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOR7WpfWBZ2BJda4w9W3qG9a986:v4J+OlfOhWppCW6G9a98Hr2 |
| MD5: | 2F6B11A7E914718E0290410E85366FE9 |
| SHA1: | 69BB69E25CA7D5EF0935317584E6153F3FD9A88C |
| SHA-256: | 05B85D96F41FFF14D8F608DAD03AB71E2C1017C2DA0914D7C59291BAD7A54F8E |
| SHA-512: | 0D40BCCAA59FEDECF7243D63B33C42592541D0330FEFC78EC81A4C6B9689922D5B211011CA4BE23AE22621CCE4C658F52A1552C92D7AC3615241EB640F8514B |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js |
| Preview: | /*! jQuery v2.2.4 \| (c) jQuery Foundation \| jquery.org/license */!.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+\|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\w-logo-blue-white-bg[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 80 x 80, 8-bit/color RGBA, non-interlaced |
| Category: | downloaded |
| Size (bytes): | 4119 |
| Entropy (8bit): | 7.949120703870044 |
| Encrypted: | false |
| SSDEEP: | 96:h3bdWfcmTY+aRF1pXWZL2+42HGhIUc8KeLEd:hgXTY+as02mOB8XLEd |
| MD5: | 000BF649CC8F6BF27CFB04D1BCDCD3C7 |
| SHA1: | D73D2F6D74EC6CDCBAE07955592962E77D8AE814 |
| SHA-256: | 6BDB369337AC2496761C6F063BFFEA0AA6A91D4662279C399071A468251F51F0 |
| SHA-512: | 73D2EA5FFC572C1AE73F37F8F0FF25E945AFEE8E077B6EE42CE969E575CDC2D8444F90848EA1CB4D1C9EE4BD725AEE2B4576AFC25F17D7295A90E1CBFE6EDFD5 |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://landarch.org/wp-includes/images/w-logo-blue-white-bg.png |
| Preview: | .PNG.....IHDR...P...P.....IDATx..].xU...[..V..*).Kk...V.k..J]jKEl?...t...!.{.,...E.....@....F.%.....B...N.y..w.....I{.o...;.s..3...WH...../.zBp.o,XW.....#Z.f...\|mvD..9..F.....y..o.....1^.743l.....v..#.c.E&.e..hU1.{...._cZ..We.v....f.w....(..6\|.Y.. I:x..-.&.....D.....<.6.6.l....T..)...\|....#..$g...VN.....!'/6.w..B.h.}....EV.....k.7" f.}.G.~#..M..+....G....iB.....]..?+.....'.j.GB..P%.....\...../..%...&.8E..."....44.J...1.....S.....d.j..]ni%._..9.{.O?.H..6T.\|A.GC..g...U.oDEt,?.0....~....q=.y.~.9.Z.....c...v.._....$.0.2...F.9a.L..)..l...2...w...I..&....Vg.....H.I..r...../....z.`..+...Z.^U.=..5aBpb..0< ../>.9.c....".I..0.3N.}}....]]Fb...Q.....W.....OQ..y;.....\|.37..}.....(c.....X..`xX).;.....<5S....>.9..G.:..=..0^.....I_<G.....H....C.O.*.....Hk{..{....]Nc..B.8..}%>..w....Z...).....\..>....c..2...&..0'.DZJ.'~{Y....I....?.....fR.a.....;.<..lRG..n.....Q.....Nf.6. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\585b051251[1].js | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with very long lines |
| Category: | downloaded |
| Size (bytes): | 10866 |
| Entropy (8bit): | 5.182623714755422 |
| Encrypted: | false |
| SSDEEP: | 192:BgHN42S+9SZRvACpiIthFzoXnemF+shSGnZ+PPxQDqv7jh81Q5l8OcchIlzbCn:WRCfhFzevnEZ/h81Q5l8OsE |
| MD5: | D8CA71772D1E86D5FB9D5E2F6CC1AE70 |
| SHA1: | 9B043E60997FE552D652E4474E16AFF923D7AA76 |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\585b051251[1].js | |
|---|---|
| SHA-256: | 7D840153F02AD6D91D652354E35B590721916D16C33956631EEF0E7D3B5613EE |
| SHA-512: | 8E9DA8E9AE10EC0EB854A6E488FB4568A960EE10AF46FE4AA49F22F227CB94997F40E49E10A81E341B99489256163A2C0E065730EEA642777061CDA61B4D56C1 |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://kit.fontawesome.com/585b051251.js |
| Preview: | window.FontAwesomeKitConfig = {"asyncLoading":{"enabled":true},"autoA11y":{"enabled":true},"baseUrl":"https://ka-f.fontawesome.com","baseUrlKit":"https://kit.fontawesome.com","detectConflictsUntil":null,"iconUploads":{},"id":132286382,"license":"free","method":"css","minify":{"enabled":true},"token":"585b051251","v4FontFaceShim":{"enabled":false},"v4shim":{"enabled":true},"version":"5.15.3"};!function(t){"function"==typeof define&&define.amd?define("kit-loader",t):t()}(function(){"use strict";function t(e){return(t="function"==typeof Symbol&&"symbol"==typeof Symbol.iterator?function(t){return typeof t}:function(t){return t&&"function"==typeof Symbol&&t.constructor===Symbol&&t!==Symbol.prototype?"symbol":typeof t})(e)}function e(t,e,n){return e in t?Object.defineProperty(t,e,{value:n,enumerable:!0,configurable:!0,writable:!0}):t[e]=n,t}function n(t,e){var n=Object.keys(t);if(Object.getOwnPropertySymbols){var r=Object.getOwnPropertySymbols(t);e&&(r=r.filter((function(e){return Object.g |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\bootstrap.min[1].css | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with very long lines |
| Category: | downloaded |
| Size (bytes): | 144877 |
| Entropy (8bit): | 5.049937202697915 |
| Encrypted: | false |
| SSDEEP: | 1536:GcoqwrUPyDHU7c7TcDEBi82NcuSELL4d/+oENM6HN26Q:VoPgPard2oENM6HN26Q |
| MD5: | 450FC463B8B1A349DF717056FBB3E078 |
| SHA1: | 895125A4522A3B10EE7ADA06EE6503587CBF95C5 |
| SHA-256: | 2C0F3DCFE93D7E380C290FE4AB838ED8CADFF1596D62697F5444BE460D1F876D |
| SHA-512: | 93BF1ED5F6D8B34F53413A86EFD4A925D578C97ABC757EA871F3F46F340745E4126C48219D2E8040713605B64A9ECF7AD986AA8102F5EA5ECF9228801D962F5D |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css |
| Preview: | /*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors. * Copyright 2011-2018 Twitter, Inc.. * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */:root{--blue:#007bff;--indigo:#6610f2;--purple:#6f42c1;--pink:#e83e8c;--red:#dc3545;--orange:#fd7e14;--yellow:#ffc107;--green:#28a745;--teal:#20c997;--cyan:#17a2b8;--white:#fff;--gray:#6c757d;--gray-dark:#343a40;--primary:#007bff;--secondary:#6c757d;--success:#28a745;--info:#17a2b8;--warning:#ffc107;--danger:#dc3545;--light:#f8f9fa;--dark:#343a40;--breakpoint-xs:0;--breakpoint-sm:576px;--breakpoint-md:768px;--breakpoint-lg:992px;--breakpoint-xl:1200px;--font-family-sans-serif:-apple-system,BlinkMacSystemFont,"Segoe UI",Roboto,"Helvetica Neue",Arial,sans-serif,"Apple Color Emoji","Segoe UI Emoji","Segoe UI Symbol";--font-family-monospace:SFMono-Regular,Menlo,Monaco,Consolas,"Liberation Mono","Courier New",monospace}*,::after,::before{box-sizing:border-box}html{font-family:sans |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\bootstrap.min[1].js | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with very long lines |
| Category: | downloaded |
| Size (bytes): | 48944 |
| Entropy (8bit): | 5.272507874206726 |
| Encrypted: | false |
| SSDEEP: | 768:9VG5R15WbHVKZrycEHSYro34CrSLB6WU/6DqBf4l1B:9VIRuo53XiwWTvl1B |
| MD5: | 14D449EB8876FA55E1EF3C2CC52B0C17 |
| SHA1: | A9545831803B1359CFEED47E3B4D6BAE68E40E99 |
| SHA-256: | E7ED36CEEE5450B4243BBC35188AFABDFB4280C7C57597001DE0ED167299B01B |
| SHA-512: | 00D9069B9BD29AD0DAA0503F341D67549CCE28E888E1AFFD1A2A45B64A4C1BC460D81CFC4751857F991F2F4FB3D2572FD97FCA651BA0C2B0255530209B182F2 |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js |
| Preview: | /*!. * Bootstrap v4.0.0 (https://getbootstrap.com). * Copyright 2011-2018 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors). * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE). */.!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function"==typeof define&&define.amd?define(["exports","jquery","popper.js"],e):e(t.bootstrap={},t.jQuery,t.Popper)}(this,function(t,e,n){"use strict";function i(t,e){for(var n=0;n<e.length;n++){var i=e[n];i.enumerable=i.enumerable||!1,i.configurable=!0,"value"in i&&(i.writable=!0),Object.defineProperty(t,i.key,i)}}function s(t,e,n){return e&&i(t.prototype,e),n&&i(t,n),t}function r(){return(r=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var i in n)Object.prototype.hasOwnProperty.call(n,i)&&(t[i]=n[i])}return t}).apply(this,arguments)}e=e&&e.hasOwnProperty("default")?e.default:e,n=n&&n.hasOwnProp |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\css[2].css | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text |
| Category: | downloaded |
| Size (bytes): | 211 |
| Entropy (8bit): | 5.026484232218891 |
| Encrypted: | false |
| SSDEEP: | 6:0IFFwKh+56ZRWHMqh7izlpdBEoKOEEJTONin:jFWmO6ZRoMqt6p3EondOY |
| MD5: | 04F7435B2672FBE66984EA436E7087C6 |
| SHA1: | 44896875E69B297EB979CC0D3E8522D872656BA8 |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\css[2].css | |
|---|---|
| SHA-256: | F9088C15A062F0C7708C3864C5E261A2E4961DFEB0F150DF744FAEC2E3B74AD6 |
| SHA-512: | 9A1D01A7FAC3D6B205CFA37C05A93AFA9D903D4D35DCB16E31D3A31D19CD65B8DE5D66E626BC7F70D07841C779E20CD2C2DD6254824F96DE0E8E576E156F17D |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://fonts.googleapis.com/css?family=Yellowtail&display=swap |
| Preview: | @font-face {. font-family: 'Yellowtail';. font-style: normal;. font-weight: 400;. font-display: swap;. src: url(https://fonts.gstatic.com/s/yellowtail/v11/OZpGg_pnoDtINPfRIlLohlvHxw.woff) format('woff');.}. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\index[1].htm | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators |
| Category: | downloaded |
| Size (bytes): | 11777 |
| Entropy (8bit): | 4.8159515725639555 |
| Encrypted: | false |
| SSDEEP: | 192:K2FI5vEJKnYmrDfG4RywAOT+UY/t4IdtWPtY:1nmRnAKyt48tZ |
| MD5: | 6D1D3C4FD92B63CC534BE0EDF3AF18DC |
| SHA1: | 5F5442FEB5BE60239F185E969C45050A7DBADE2A |
| SHA-256: | 65ADCB045AEFB4D0028A6AF36EC9D42BBD4DAE9AFF2CF85810BB4A6F44D4B25C |
| SHA-512: | 2D42684CF0A44E262C958172C2446974A4AE9B8D17F7208A5FCB690964EE0D56FEB157B9AB6166B8F94FBDCBA027271C36B66784655E8FD96CE0B5522FE71AA |
| Malicious: | **true** |
| Yara Hits: | • Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\index[1].htm, Author: Joe Security<br>• Rule: JoeSecurity_HtmlPhish_7, Description: Yara detected HtmlPhish_7, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\index[1].htm, Author: Joe Security |
| Reputation: | low |
| IE Cache URL: | http://https://landarch.org/hassani/index.php |
| Preview: | ...<!doctype html>..<html lang="en">..<head>.. <script src="https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>.. <script src="https://code.jquery.com/jquery-3.1.1.min.js">.. <script src="https://code.jquery.com/jquery-3.3.1.js" integrity="sha256-2Kok7MbOyxpgUVvAk/HJ2jigOSYS2auK4Pfzbm7uH60=" crossorigin="anonymous"></script>.. Required meta tags -->.. <meta charset="utf-8">.. <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">.... Bootstrap CSS -->.. <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css" integrity="sha384-Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/dAiS6JXm" crossorigin="anonymous">.. <link href="https://fonts.googleapis.com/css?family=Yellowtail&display=swap" rel="stylesheet">.. <script src="https://kit.fontawesome.com/585b051251.js" crossorigin="anonymous"></script>.. <title>Share Point Online</title>.. <link |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\popper.min[1].js | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with very long lines |
| Category: | downloaded |
| Size (bytes): | 19188 |
| Entropy (8bit): | 5.212814407014048 |
| Encrypted: | false |
| SSDEEP: | 384:+CbuG4xGNoDic2UjKPafxwC5b/4xQviOJU7QzxzivDdE3pcGdjkd/9jt3B+Kb964:zb4xGmiJfaf7gxQvVU7eziv+cSjknZ3f |
| MD5: | 70D3FDA195602FE8B75E0097EED74DDE |
| SHA1: | C3B977AA4B8DFB69D651E07015031D385DED964B |
| SHA-256: | A52F7AA54D7BCAAFA056EE0A050262DFC5694AE28DEE8B4CAC3429AF37FF0D66 |
| SHA-512: | 51AFFB5A8CFD2F93B473007F6987B19A0A1A0FB970DDD59EF45BD77A355D82ABBBD60468837A09823496411E797F05B1F962AE93C725ED4C00D514BA40269D1 |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js |
| Preview: | /*. Copyright (C) Federico Zivolo 2017. Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT).. */(function(e,t){'object'==typeof exports&&'undefined'!=typeof module?module.exports=t():'function'==typeof define&&define.amd?define(t):e.Popper=t()})(this,function(){'use strict';function e(e){return e&&'[object Function]'==={}.toString.call(e)}function t(e,t){if(1!==e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e){return'HTML'===e.nodeName?e:e.parentNode||e.host}function n(e){if(!e)return document.body;switch(e.nodeName){case'HTML':case'BODY':return e.ownerDocument.body;case'#document':return e.body;}var i=t(e),r=i.overflow,p=i.overflowX,s=i.overflowY;return /(auto|scroll)/.test(r+s+p)?e:n(o(e))}function r(e){var o=e&&e.offsetParent,i=o&&o.nodeName;return i&&'BODY'!==i&&'HTML'!==i?-1!==['TD','TABLE'].indexOf(o.nodeName)&&'static'===t(o,'position')?r(o):o:e?e.ownerDocument.documentElement:document.documentElement}functio |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\8[1].jpg | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | [TIFF image data, big-endian, direntries=12, height=709, bps=0, PhotometricIntepretation=RGB, orientation=upper-left, width=1200], baseline, precision 8, 1200x646, frames 3 |
| Category: | downloaded |
| Size (bytes): | 161118 |
| Entropy (8bit): | 7.5594351594508185 |
| Encrypted: | false |
| SSDEEP: | 3072:WucfAcwuKGuN2q/gSsqnk4br5XUGpppLqfmazv7l04J:OMuKbYOF355XEuAv7lnJ |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\8[1].jpg | |
|---|---|
| MD5: | F17B5B1163EFB6D2D47DE6BAE6D3A9CD |
| SHA1: | 6D6964B34BC44C6D2B106ADE1AE675985B96D012 |
| SHA-256: | 7829F065E0E10C8466F3D57766E0719421B7B652F6A1082F21B98702F1B28A30 |
| SHA-512: | 7C0CBEF1D3CAE66A18C74544E593803C2EEC56817E762A385D54437BC7D597B2598886B0C0EDF72C6E934E9F146CEFC89392A492DB5425A1071E61CA1F15685 |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://landarch.org/hassani/images/8.jpg |
| Preview: | .....Exif..MM.*.....(.....1.....".....2.....i.....$.....'.....'.Adobe Photoshop CC 2015 (Windows).2020:01:21 13:41:42.....0221.....r.....z.(.....%.....H.....H.....Adobe_CM.....Adobe.d.....V...".....?.....3.....!.1.AQa."q.2....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?.....q..KJG..x.."....]..TX...[^.m...R.....X.5..j?p.A.RI%0...MN.$..@.4 |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\jquery-3.1.1.min[1].js | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with very long lines |
| Category: | downloaded |
| Size (bytes): | 86709 |
| Entropy (8bit): | 5.367391365596119 |
| Encrypted: | false |
| SSDEEP: | 1536:9NhEyjjTikEJO4edXXe9J578go6MWXqcVhrLyB4Lw13sh2bzrl1+iuH7U3gBORDT:jxcq0hrLZwpsYbmzORDU8Cu5 |
| MD5: | E071ABDA8FE61194711CFC2AB99FE104 |
| SHA1: | F647A6D37DC4CA055CED3CF64BBC1F490070ACBA |
| SHA-256: | 85556761A8800D14CED8FCD41A6B8B26BF012D44A318866C0D81A62092EFD9BF |
| SHA-512: | 53A2B560B20551672FBB0E6E72632D4FD1C7E2DD2ECF7337EBAAAB179CB8BE7C87E9D803CE7765706BC7FCBCF993C34587CD1237DE5A279AEA19911D69067E65 |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://code.jquery.com/jquery-3.1.1.min.js |
| Preview: | /*! jQuery v3.1.1 \| (c) jQuery Foundation \| jquery.org/license */.!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,m=l.toString,n=m.call(Object),o={};function p(a,b){b=b\|\|d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.1.1",r=function(a,b){return new r.fn.init(a,b)},s=/^[\s\uFEFF\xA0]+\|[\s\uFEFF\xA0]+$/g,t=/^-ms-/,u=/-([a-z])/g,v=function(a,b){return b.toUpperCase()};r.fn=r.prototype={jquery:q,constructor:r,length:0,toArray:function(){return f.call(this)},get:function(a){return null==a?f.call(this):a<0?this[a+this.length]:this[a]},pushStack:function(a){var b=r.merge(this.con |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\jquery-3.2.1.slim.min[1].js | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text, with very long lines |
| Category: | downloaded |
| Size (bytes): | 69597 |
| Entropy (8bit): | 5.369216080582935 |
| Encrypted: | false |
| SSDEEP: | 1536:qNhEyjjTikEJO4edXXe9J578go6MWX2xkjVe4c4j2ll2Ac7pK3F71QDU8CuT:Exc2yjq4j2uYnQDU8CuT |
| MD5: | 5F48FC77CAC90C4778FA24EC9C57F37D |
| SHA1: | 9E89D1515BC4C371B86F4CB1002FD8E377C1829F |
| SHA-256: | 9365920887B11B33A3DC4BA28A0F93951F200341263E3B9CEFD384798E4BE398 |
| SHA-512: | CAB8C4AFA1D8E3A8B7856EE29AE92566D44CEEAD70C8D533F2C98A976D77D0E1D314719B5C6A473789D8C6B21EBB4B89A6B0EC2E1C9C618FB1437EBC77D3A269 |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://code.jquery.com/jquery-3.2.1.slim.min.js |
| Preview: | /*! jQuery v3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_evalUrl,-event/ajax,-effects,-effects/Tween,-effects/animatedSelector \| (c) JS Foundation and other contributors \| jquery.org/license */.!function(a,b){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){"use strict";var c=[],d=a.document,e=Object.getPrototypeOf,f=c.slice,g=c.concat,h=c.push,i=c.indexOf,j={},k=j.toString,l=j.hasOwnProperty,n=m.call(Object),o={};function p(a,b){b=b\|\|d;var c=b.createElement("script");c.text=a,b.head.appendChild(c).parentNode.removeChild(c)}var q="3.2.1 -ajax,-ajax/jsonp,-ajax/load,-ajax/parseXML,-ajax/script,-ajax/var/location,-ajax/var/nonce,-ajax/var/rquery,-ajax/xhr,-manipulation/_e |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\gmail[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 1280 x 1280, 8-bit/color RGBA, non-interlaced |
| Category: | downloaded |
| Size (bytes): | 66743 |
| Entropy (8bit): | 7.712342056984168 |
| Encrypted: | false |
| SSDEEP: | 1536:FxqKcVqezl0vLoYxEuKoYk5LHjGkT3b1mQOEj0+R+EH:FsK2qezl0zoYxEuKo7CYrOb+Rb |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\gmail[1].png | |
|---|---|
| MD5: | DCE2F2B0E50CB1DBB0246D152791CB46 |
| SHA1: | D0A69C159304EDC08DB005163E7A0DAF5A1E98A6 |
| SHA-256: | ACF087C1757F08B0CFD53D59066544D7EF0BFCC50999E77C5813739CD9DC1479 |
| SHA-512: | 91054B36EF1673B24E4FE3DC324CBE339F4E9EB72785A6A4C355C7B2A11A9A7C6E188FF9BF5B34FFDD2805D4BBED71EF6CA4975EE3E330FD8D8E383ED64B28EE |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://landarch.org/hassani/images/gmail.png |
| Preview: | .PNG.....IHDR.....sBIT....\|.d.....pHYs...../....tEXtSoftware.www.inkscape.org..<... .IDATx...{x.u.....I.sS..9Q(..J.L&.$..V\|.....#..''...Zw.eEQv.Q..U.A]9Vh..I8...H2)`....i.....).....f.y....L.pu...{n..... .....@Is..... mj=...X<65....U.l.b.t.U...mR...e..P.i.$.i2U..@N1.f...i.s...cf. ../....2ev.`..%.\|.o...s..j..l.B....V&..s;b..Pfg.....!...:..5....$.@...I0.=.lY.....a...B.4g... T.9Wif..R..o.R.t'.0...?G.9i...L...*..&..s.Vgnkhn...;p[.0.5.....$.....P.....^''.HL.M...@.p..;04....9.&.(i....9.sK..=&.'$m.....f..1..'...f2.Uww.....PH....@..xq....k.2..l.Luf..s5..`.\| |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\hover[1].css | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | ASCII text |
| Category: | downloaded |
| Size (bytes): | 114697 |
| Entropy (8bit): | 4.9296726009523 |
| Encrypted: | false |
| SSDEEP: | 1536:67O7EesvXIPRX4PT8aZv8qoXIoqbTFaFeTxvyAZ+D7M71D:qXIPRX4PT3 |
| MD5: | FAC4178C15E5A86139C662DAFC809501 |
| SHA1: | EF1481841399156A880EC31B07DDA9CFAA1ACE39 |
| SHA-256: | BB88454962767EB6F2DDB1AABAAF844D8A57DE7E8F848D7F6928F81B54998452 |
| SHA-512: | 0902219B6E236FBF9D8173D1D452C8733C1BF67B0EB906CC9866EA0C27C2D08F6DA556D01475E9B54E2C6CE797B230BFBD5F39055CE0C71EA4D3E36872C3789 |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://landarch.org/hassani/css/hover.css |
| Preview: | /*!. * Hover.css (http://ianlunn.github.io/Hover/). * Version: 2.3.2. * Author: Ian Lunn @IanLunn. * Author URL: http://ianlunn.co.uk/. * Github: https://github.com/IanLunn/Hover.. * Hover.css Copyright Ian Lunn 2017. Generated with Sass.. */./* 2D TRANSITIONS */./* Grow */..hvr-grow {. display: inline-block;. vertical-align: middle;. -webkit-transform: perspective(1px) translateZ(0);. transform: perspective(1px) translateZ(0);. box-shadow: 0 0 1px rgba(0, 0, 0, 0);. -webkit-transition-duration: 0.3s;. transition-duration: 0.3s;. -webkit-transition-property: transform;. transition-property: transform;.}..hvr-grow:hover, .hvr-grow:focus, .hvr-grow:active {. -webkit-transform: scale(1.1);. transform: scale(1.1);.}../* Shrink */..hvr-shrink {. display: inline-block;. vertical-align: middle;. -webkit-transform: perspective(1px) translateZ(0);. transform: perspective(1px) translateZ(0);. box-shadow: 0 0 1px rgba(0, 0, 0, 0);. -webkit-transition-duration: 0.3s;. transition- |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\office3651[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 187 x 188, 8-bit/color RGBA, non-interlaced |
| Category: | downloaded |
| Size (bytes): | 18025 |
| Entropy (8bit): | 3.011161251318808 |
| Encrypted: | false |
| SSDEEP: | 96:2S+WvkiqJq6Uq7NXrNG+GHhsc5yeFZV9D2Ydcx/NTV0K0VFDsCmm:2SJkiOq6Uq75shDs1kFP |
| MD5: | FE22440D79FFA34950F512EF4A718B2A |
| SHA1: | 0E147E59544EE6580D3095353D4420849FA5EB8A |
| SHA-256: | A2F26B68A6C8810C1AEB4048C938F835A86BA83756A7A440F989B967E78F3BA8 |
| SHA-512: | 64218ECD4140DC05E50EB7BA4C9813794B8B5A4310C8308244205BA6ADA8EE7C2D1840121730A00800E41775241D8AFA02125A966064CD0EB2CC7D3E4605B81 |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://landarch.org/hassani/images/office3651.png |
| Preview: | .PNG.....IHDR..... .....pHYs.....<eiTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?>.<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 ">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/". xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#". xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/". xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/">. <xmp:CreatorTool>Adobe Photoshop CC 2015 (Windows)</xmp:CreatorTool>. <xmp:CreateDate>2020-01-18T21:49:38+05:00</xmp:CreateDate>. <xmp:MetadataDate>2020-01-21T14:30:14+05:00</xmp:MetadataDate>. <x |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\other1[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 190 x 187, 8-bit/color RGBA, non-interlaced |
| Category: | downloaded |
| Size (bytes): | 21882 |
| Entropy (8bit): | 4.268463452779894 |
| Encrypted: | false |
| SSDEEP: | 192:ESCkiDw7e9Mg/wio0EYm9FWyo2XdJfXoOZdEDfmiIJQdiRVi/WTanY:DBiDw7eAdq+FWyo2/fXoZbDlJ0ci/BnY |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\other1[1].png | |
|---|---|
| MD5: | 6843A244E12FAB158AA189680B5E7049 |
| SHA1: | 0E1C691F87CC4FA35C88344974F2829C40176B70 |
| SHA-256: | 3A9B144D6482B78AFC4E0A940A1D3C22240F14FA535B808CF4DAB9635339569F |
| SHA-512: | 145010C45B6B83EA4005EB367C0507959FF0817E482F19E9973504081ACAE1B7827CBD1172CEC7732B13F4E0CEC058271BD6700444FBCF61FB6A3C068A3744C4 |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://landarch.org/hassani/images/other1.png |
| Preview: | .PNG.....IHDR.....$.... cHRM..z&.....u0...`..:....p..Q<....sRGB.....gAMA.....a.....pHYs.....:.iTXtXML:com.adobe.xmp.....<?xpacket begin="." id=" W5M0MpCehiHzreSzNTczkc9d"?>.<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 ">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:xmpMM= "http://ns.adobe.com/xap/1.0/mm/". xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#". xmlns:photoshop="http://ns.adobe.com/ph otoshop/1.0/". xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:tiff="http://ns.adobe.com/tiff/1.0/". xmlns:exif="http://ns.adobe.com/exif/1.0/">. <xmp:CreatorTool>Adobe Photoshop CC 2015 (Windows)</xmp:CreatorTool>. <xmp:CreateDate>2020-01-18T21:59:57+05:00</xmp:CreateDate>. < |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\outlook1[1].png | |
|---|---|
| Process: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| File Type: | PNG image data, 26 x 26, 8-bit/color RGBA, non-interlaced |
| Category: | downloaded |
| Size (bytes): | 771 |
| Entropy (8bit): | 7.682244426935498 |
| Encrypted: | false |
| SSDEEP: | 24:74yiH9yQmOntihdLl00qDeu1BcaDa0oljZG0:omOntO7v/uJDYG0 |
| MD5: | C3FC46C5799C76F9107504028F39190F |
| SHA1: | 519096AD3F03410CF9CE3C9B9FCCA6B439D97B23 |
| SHA-256: | 57898461712A639D119BDF88B7145919DCC8956C7A271D2E4A1084B29EAE6785 |
| SHA-512: | DF4A0A2F78B2013035FB738BF405119B275D4CFEC31A23071EB9AF499D5F31FDC4BE22754CE791C975D7D417E908B5CAD16F962B0ADD3DFDCDE19844D74F668 |
| Malicious: | false |
| Reputation: | low |
| IE Cache URL: | http://https://landarch.org/hassani/images/outlook1.png |
| Preview: | .PNG.....IHDR.....JL.....bKGD.....IDATH....k.A..k6.b.F1..H@...j@.aQ...(.. .. ..... .A..D...I.....E.....1...W...;;.Y.d.}].U5]..x"3?....!..A..y..+R2\...m.NX.=..p.0... d.^.3.....J.Z.X.).....P\..x1.3.M.0....m.....F....?...n.....I.Fo)x._ R|.s..a.T?...?.=.9.Y..u....z..|.....Wz...h..<..P.. ...$.Y.....k`/4.y/.....L.C....."....U....7....G...'h.....1j1E..%t..... @..a.....b.ED-.Tn.<..o.D...o..(.{1l>.....".4a.:k.l./.7t./.Q-'..>.. .....'3eb..d.@=4...C....A...;..N.X3.(.....,v...+...S...W..l...@,...j.).u<..@u..0...V&.b.yp.....0..o.?..V..B =.~&m"r (...6;EP.T.....h.m".[f.U)|t..2.Q.....g.cP.W...D..[.O>..d;.yI.{/..#v.._..$.Q.....t\E..5i.q._.."/n...v.w..Uo ...#..S....^.....F..+._??.r.....IEND.B`. |

| C:\Users\user\AppData\Local\Temp\~DF21461B56EB5BEA2A.TMP | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 35185 |
| Entropy (8bit): | 0.4666697127888211 |
| Encrypted: | false |
| SSDEEP: | 48:kBqoxKAuvScS+yU+X7I70Rh4ivuQbif5ag0b:kBqoxKAuvScS+yU+XkYwsb |
| MD5: | A4938E1204708E36FF2E8628BCB87CF5 |
| SHA1: | 83BAF1E841165C411818A6F324E30EA0C5C38628 |
| SHA-256: | AC0FF52D2C03BBE66178F80902151DCFF5161D89204FD358F42785E49330E035 |
| SHA-512: | 8C95DB7BC00CC88E3198E4AED698323F81BE533EB7243EFCF425D304E86F62DA23400BBBDAE13CED1A7C75B47117EA6FFD10A786EE1A396F87298E1FACEE8E9E |
| Malicious: | false |
| Reputation: | low |
| Preview: | .....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ..... ..... ..... ..... |

| C:\Users\user\AppData\Local\Temp\~DF4E7BFA20179A1DA0.TMP | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 25441 |
| Entropy (8bit): | 0.27918767598683664 |
| Encrypted: | false |
| SSDEEP: | 24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab |
| MD5: | AB889A32AB9ACD33E816C2422337C69A |
| SHA1: | 1190C6B34DED2D295827C2A88310D10A8B90B59B |
| SHA-256: | 4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA |

| C:\Users\user\AppData\Local\Temp\~DF4E7BFA20179A1DA0.TMP | |
|---|---|
| SHA-512: | BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB |
| Malicious: | false |
| Reputation: | low |
| Preview: | .....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ..... ..... ..... ..... |

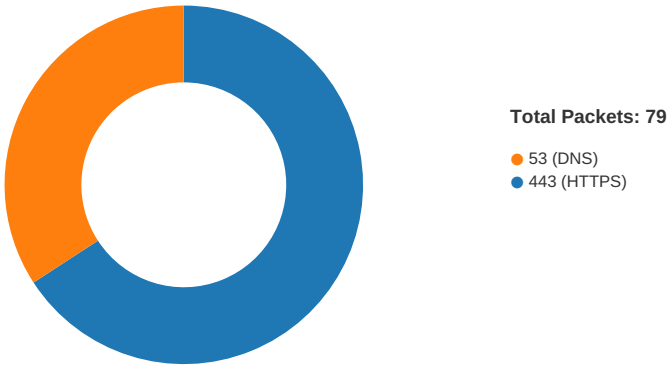
| C:\Users\user\AppData\Local\Temp\~DFC5762E6EF0DB105B.TMP | |
|---|---|
| Process: | C:\Program Files\internet explorer\iexplore.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 13029 |
| Entropy (8bit): | 0.477104916684086 |
| Encrypted: | false |
| SSDEEP: | 24:c9lLh9lLh9lIn9lIn9loO9lo+9lW/1Fg1e0O0:kBqolJf/l0 |
| MD5: | FA34330217A075959D4CF4F6BA1B9512 |
| SHA1: | FBC3F8067DAFBB318E71FF2367068ABB132A52D1 |
| SHA-256: | 6B03DA729C5B0656BDF3959B2143D78BD12C31BD7FD911943873D10884AC1609 |
| SHA-512: | 3CDDA46CAAAC75932D8F48307F2EBED334C8845E9269B9AA0C7F9780E3175AEA68876382EA0AAE3B29A06EE2D71909CDDCB19FB4B96D480C71E9DD06B688D9A |
| Malicious: | false |
| Reputation: | low |
| Preview: | .....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ..... ..... ..... ..... |

# Static File Info

## No static file info

# Network Behavior

## Network Port Distribution




## TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 12, 2021 18:52:33.896075010 CEST | 49694 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:33.896363974 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.080955982 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 12, 2021 18:52:34.080991983 CEST | 443 | 49694 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.081165075 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.081193924 CEST | 49694 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.089230061 CEST | 49694 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.089344978 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.273833036 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.273925066 CEST | 443 | 49694 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.275259018 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.275279045 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.275295973 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.275369883 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.275408030 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.275819063 CEST | 443 | 49694 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.275837898 CEST | 443 | 49694 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.275847912 CEST | 443 | 49694 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.275897026 CEST | 49694 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.275935888 CEST | 49694 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.311212063 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.311655998 CEST | 49694 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.317972898 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.318156958 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.318312883 CEST | 49694 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.496459007 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.496486902 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.496541977 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.496571064 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.496943951 CEST | 443 | 49694 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.497067928 CEST | 443 | 49694 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.497957945 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.497977972 CEST | 49694 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.498008013 CEST | 49694 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.498013973 CEST | 49694 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.502808094 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.502986908 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.503088951 CEST | 443 | 49694 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.503186941 CEST | 49694 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.547703028 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.637921095 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.637970924 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.637991905 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.638045073 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.638084888 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.682459116 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.723565102 CEST | 443 | 49694 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:34.814682961 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.815598011 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.877872944 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.890523911 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.892174959 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.892481089 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:34.894782066 CEST | 49703 | 443 | 192.168.2.6 | 104.18.10.207 |
| May 12, 2021 18:52:34.899092913 CEST | 49704 | 443 | 192.168.2.6 | 104.18.10.207 |
| May 12, 2021 18:52:34.937747955 CEST | 443 | 49703 | 104.18.10.207 | 192.168.2.6 |
| May 12, 2021 18:52:34.937889099 CEST | 49703 | 443 | 192.168.2.6 | 104.18.10.207 |
| May 12, 2021 18:52:34.941608906 CEST | 443 | 49704 | 104.18.10.207 | 192.168.2.6 |
| May 12, 2021 18:52:34.941690922 CEST | 49704 | 443 | 192.168.2.6 | 104.18.10.207 |
| May 12, 2021 18:52:34.977313995 CEST | 49705 | 443 | 192.168.2.6 | 104.16.19.94 |
| May 12, 2021 18:52:34.978410006 CEST | 49706 | 443 | 192.168.2.6 | 104.16.19.94 |
| May 12, 2021 18:52:35.000067949 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:35.000472069 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:35.004112959 CEST | 49704 | 443 | 192.168.2.6 | 104.18.10.207 |
| May 12, 2021 18:52:35.004261017 CEST | 49703 | 443 | 192.168.2.6 | 104.18.10.207 |
| May 12, 2021 18:52:35.005530119 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:35.005569935 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 12, 2021 18:52:35.005594015 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:35.005620003 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:35.005645990 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:35.005654097 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:35.005671978 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:35.005696058 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:35.005700111 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:35.005724907 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:35.005747080 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:35.005759001 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:35.005773067 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:35.005795002 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:35.005796909 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:35.005820990 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:35.005824089 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:35.005861998 CEST | 49695 | 443 | 192.168.2.6 | 50.87.140.26 |
| May 12, 2021 18:52:35.018332958 CEST | 443 | 49705 | 104.16.19.94 | 192.168.2.6 |
| May 12, 2021 18:52:35.018445969 CEST | 49705 | 443 | 192.168.2.6 | 104.16.19.94 |
| May 12, 2021 18:52:35.019330025 CEST | 443 | 49706 | 104.16.19.94 | 192.168.2.6 |
| May 12, 2021 18:52:35.019422054 CEST | 49706 | 443 | 192.168.2.6 | 104.16.19.94 |
| May 12, 2021 18:52:35.037597895 CEST | 49705 | 443 | 192.168.2.6 | 104.16.19.94 |
| May 12, 2021 18:52:35.044770956 CEST | 443 | 49704 | 104.18.10.207 | 192.168.2.6 |
| May 12, 2021 18:52:35.044852972 CEST | 443 | 49703 | 104.18.10.207 | 192.168.2.6 |
| May 12, 2021 18:52:35.047192097 CEST | 443 | 49703 | 104.18.10.207 | 192.168.2.6 |
| May 12, 2021 18:52:35.047231913 CEST | 443 | 49703 | 104.18.10.207 | 192.168.2.6 |
| May 12, 2021 18:52:35.047297001 CEST | 49703 | 443 | 192.168.2.6 | 104.18.10.207 |
| May 12, 2021 18:52:35.047326088 CEST | 49703 | 443 | 192.168.2.6 | 104.18.10.207 |
| May 12, 2021 18:52:35.047672987 CEST | 443 | 49704 | 104.18.10.207 | 192.168.2.6 |
| May 12, 2021 18:52:35.047703981 CEST | 443 | 49704 | 104.18.10.207 | 192.168.2.6 |
| May 12, 2021 18:52:35.047761917 CEST | 49704 | 443 | 192.168.2.6 | 104.18.10.207 |
| May 12, 2021 18:52:35.047790051 CEST | 49704 | 443 | 192.168.2.6 | 104.18.10.207 |
| May 12, 2021 18:52:35.077148914 CEST | 443 | 49695 | 50.87.140.26 | 192.168.2.6 |
| May 12, 2021 18:52:35.078497887 CEST | 443 | 49705 | 104.16.19.94 | 192.168.2.6 |

## UDP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 12, 2021 18:52:22.813859940 CEST | 52157 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:22.865120888 CEST | 53 | 52157 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:24.520298004 CEST | 61182 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:24.583796978 CEST | 53 | 61182 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:25.346510887 CEST | 55673 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:25.397402048 CEST | 53 | 55673 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:26.443058968 CEST | 57773 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:26.494609118 CEST | 53 | 57773 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:27.327680111 CEST | 59986 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:27.389646053 CEST | 53 | 59986 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:28.671608925 CEST | 52478 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:28.729116917 CEST | 53 | 52478 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:30.200932980 CEST | 58931 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:30.249725103 CEST | 53 | 58931 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:31.530558109 CEST | 57725 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:31.582124949 CEST | 53 | 57725 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:32.348900080 CEST | 49283 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:32.410296917 CEST | 53 | 49283 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:32.718630075 CEST | 58377 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:32.767369986 CEST | 53 | 58377 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:33.827748060 CEST | 55074 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:33.884958982 CEST | 53 | 55074 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:33.983454943 CEST | 54513 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:34.035346985 CEST | 53 | 54513 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:34.724417925 CEST | 62044 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:34.737781048 CEST | 63791 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:34.764658928 CEST | 64267 | 53 | 192.168.2.6 | 8.8.8.8 |

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 12, 2021 18:52:34.784437895 CEST | 53 | 62044 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:34.789449930 CEST | 53 | 63791 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:34.811233997 CEST | 49448 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:34.826621056 CEST | 53 | 64267 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:34.876354933 CEST | 53 | 49448 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:34.877696037 CEST | 60342 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:34.912580013 CEST | 61346 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:34.937086105 CEST | 53 | 60342 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:34.969789028 CEST | 53 | 61346 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:36.555056095 CEST | 51774 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:36.604015112 CEST | 53 | 51774 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:38.327814102 CEST | 56023 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:38.379431009 CEST | 53 | 56023 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:39.251411915 CEST | 58384 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:39.301255941 CEST | 53 | 58384 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:40.156485081 CEST | 60261 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:40.205343962 CEST | 53 | 60261 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:41.090174913 CEST | 56061 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:41.141803980 CEST | 53 | 56061 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:42.491771936 CEST | 58336 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:42.543407917 CEST | 53 | 58336 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:43.594634056 CEST | 53781 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:43.644851923 CEST | 53 | 53781 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:49.575525045 CEST | 54064 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:49.627125025 CEST | 53 | 54064 | 8.8.8.8 | 192.168.2.6 |
| May 12, 2021 18:52:51.321430922 CEST | 52811 | 53 | 192.168.2.6 | 8.8.8.8 |
| May 12, 2021 18:52:51.378710985 CEST | 53 | 52811 | 8.8.8.8 | 192.168.2.6 |

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| May 12, 2021 18:52:33.827748060 CEST | 192.168.2.6 | 8.8.8.8 | 0x1e07 | Standard query (0) | landarch.org | A (IP address) | IN (0x0001) |
| May 12, 2021 18:52:34.737781048 CEST | 192.168.2.6 | 8.8.8.8 | 0x3080 | Standard query (0) | code.jquery.com | A (IP address) | IN (0x0001) |
| May 12, 2021 18:52:34.764658928 CEST | 192.168.2.6 | 8.8.8.8 | 0xa683 | Standard query (0) | maxcdn.bootstrapcdn.com | A (IP address) | IN (0x0001) |
| May 12, 2021 18:52:34.877696037 CEST | 192.168.2.6 | 8.8.8.8 | 0x7f51 | Standard query (0) | kit.fontawesome.com | A (IP address) | IN (0x0001) |
| May 12, 2021 18:52:34.912580013 CEST | 192.168.2.6 | 8.8.8.8 | 0xfd40 | Standard query (0) | cdnjs.cloudflare.com | A (IP address) | IN (0x0001) |
| May 12, 2021 18:52:36.555056095 CEST | 192.168.2.6 | 8.8.8.8 | 0x5b9a | Standard query (0) | ka-f.fontawesome.com | A (IP address) | IN (0x0001) |
| May 12, 2021 18:52:51.321430922 CEST | 192.168.2.6 | 8.8.8.8 | 0xe136 | Standard query (0) | landarch.org | A (IP address) | IN (0x0001) |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| May 12, 2021 18:52:33.884958982 CEST | 8.8.8.8 | 192.168.2.6 | 0x1e07 | No error (0) | landarch.org | | 50.87.140.26 | A (IP address) | IN (0x0001) |
| May 12, 2021 18:52:34.789449930 CEST | 8.8.8.8 | 192.168.2.6 | 0x3080 | No error (0) | code.jquery.com | cds.s5x3j6q5.hwcdn.net | | CNAME (Canonical name) | IN (0x0001) |
| May 12, 2021 18:52:34.826621056 CEST | 8.8.8.8 | 192.168.2.6 | 0xa683 | No error (0) | maxcdn.bootstrapcdn.com | | 104.18.10.207 | A (IP address) | IN (0x0001) |
| May 12, 2021 18:52:34.826621056 CEST | 8.8.8.8 | 192.168.2.6 | 0xa683 | No error (0) | maxcdn.bootstrapcdn.com | | 104.18.11.207 | A (IP address) | IN (0x0001) |
| May 12, 2021 18:52:34.937086105 CEST | 8.8.8.8 | 192.168.2.6 | 0x7f51 | No error (0) | kit.fontawesome.com | kit.fontawesome.com.cdn.cloudflare.net | | CNAME (Canonical name) | IN (0x0001) |
| May 12, 2021 18:52:34.969789028 CEST | 8.8.8.8 | 192.168.2.6 | 0xfd40 | No error (0) | cdnjs.cloudflare.com | | 104.16.19.94 | A (IP address) | IN (0x0001) |
| May 12, 2021 18:52:34.969789028 CEST | 8.8.8.8 | 192.168.2.6 | 0xfd40 | No error (0) | cdnjs.cloudflare.com | | 104.16.18.94 | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| May 12, 2021 18:52:36.604015112 CEST | 8.8.8.8 | 192.168.2.6 | 0x5b9a | No error (0) | ka-f.fontawesome.com | ka-f.fontawesome.com.cdn.cloudflare.net | | CNAME (Canonical name) | IN (0x0001) |
| May 12, 2021 18:52:51.378710985 CEST | 8.8.8.8 | 192.168.2.6 | 0xe136 | No error (0) | landarch.org | | 50.87.140.26 | A (IP address) | IN (0x0001) |

## HTTPS Packets

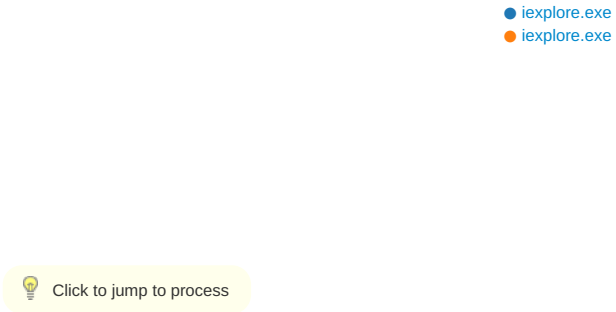
| Timestamp | Source IP | Source Port | Dest IP | Dest Port | Subject | Issuer | Not Before | Not After | JA3 SSL Client Fingerprint | JA3 SSL Client Digest |
|---|---|---|---|---|---|---|---|---|---|---|
| May 12, 2021 18:52:34.275295973 CEST | 50.87.140.26 | 443 | 192.168.2.6 | 49695 | CN=cpcontacts.landarch.org CN=R3, O=Let's Encrypt, C=US | CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co. | Sun May 02 08:27:37 CEST 2021 | Sat Jul 31 08:27:37 CEST 2021 | 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=R3, O=Let's Encrypt, C=US | CN=DST Root CA X3, O=Digital Signature Trust Co. | Wed Oct 07 21:21:40 CEST 2020 | Wed Sep 29 21:21:40 CEST 2021 | | |
| May 12, 2021 18:52:34.275847912 CEST | 50.87.140.26 | 443 | 192.168.2.6 | 49694 | CN=cpcontacts.landarch.org CN=R3, O=Let's Encrypt, C=US | CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co. | Sun May 02 08:27:37 CEST 2021 | Sat Jul 31 08:27:37 CEST 2021 | 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=R3, O=Let's Encrypt, C=US | CN=DST Root CA X3, O=Digital Signature Trust Co. | Wed Oct 07 21:21:40 CEST 2020 | Wed Sep 29 21:21:40 CEST 2021 | | |
| May 12, 2021 18:52:35.047231913 CEST | 104.18.10.207 | 443 | 192.168.2.6 | 49703 | CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US | CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE | Mon Mar 01 01:00:00 CET 2021 | Tue Mar 01 00:59:59 CET 2022 | 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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US | CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE | Mon Jan 27 13:48:08 CET 2020 | Wed Jan 01 00:59:59 CET 2025 | | |
| May 12, 2021 18:52:35.047703981 CEST | 104.18.10.207 | 443 | 192.168.2.6 | 49704 | CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US | CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE | Mon Mar 01 01:00:00 CET 2021 | Tue Mar 01 00:59:59 CET 2022 | 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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US | CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE | Mon Jan 27 13:48:08 CET 2020 | Wed Jan 01 00:59:59 CET 2025 | | |
| May 12, 2021 18:52:35.080284119 CEST | 104.16.19.94 | 443 | 192.168.2.6 | 49705 | CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US | CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE | Wed Oct 21 02:00:00 CEST 2020 | Thu Oct 21 01:59:59 CEST 2021 | 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 |
| | | | | | | | Mon Jan 27 13:48:08 CET 2020 | Wed Jan 01 00:59:59 CET 2025 | | |

| Timestamp | Source IP | Source Port | Dest IP | Dest Port | Subject | Issuer | Not Before | Not After | JA3 SSL Client Fingerprint | JA3 SSL Client Digest |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US | CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE | Mon Jan 27 13:48:08 CET 2020 | Wed Jan 01 00:59:59 CET 2025 | | |
| May 12, 2021 18:52:35.277688980 CEST | 104.16.19.94 | 443 | 192.168.2.6 | 49706 | CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US | CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE | Wed Oct 21 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020 | Thu Oct 21 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2025 | 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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US | CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE | Mon Jan 27 13:48:08 CET 2020 | Wed Jan 01 00:59:59 CET 2025 | | |
| May 12, 2021 18:52:51.763799906 CEST | 50.87.140.26 | 443 | 192.168.2.6 | 49718 | CN=cpcontacts.landarch.org CN=R3, O=Let's Encrypt, C=US | CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co. | Sun May 02 08:27:37 CEST 2021 Wed Oct 07 21:21:40 CEST 2020 | Sat Jul 31 08:27:37 CEST 2021 Wed Sep 29 21:21:40 CEST 2021 | 771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0 | 37f463bf4616ecd445d4a1937da06e19 |
| | | | | | CN=R3, O=Let's Encrypt, C=US | CN=DST Root CA X3, O=Digital Signature Trust Co. | Wed Oct 07 21:21:40 CEST 2020 | Wed Sep 29 21:21:40 CEST 2021 | | |

## Code Manipulations

## Statistics

### Behavior




## System Behavior

## Analysis Process: iexplore.exe PID: 1972 Parent PID: 792

### General

| | |
|---|---|
| Start time: | 18:52:31 |
| Start date: | 12/05/2021 |
| Path: | C:\Program Files\internet explorer\iexplore.exe |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding |
| Imagebase: | 0x7ff721e20000 |
| File size: | 823560 bytes |
| MD5 hash: | 6465CB92B25A7BC1DF8E01D8AC5E7596 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

### 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 |
|---|---|---|---|---|---|---|---|

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

## Analysis Process: iexplore.exe PID: 5784 Parent PID: 1972

### General

| | |
|---|---|
| Start time: | 18:52:32 |
| Start date: | 12/05/2021 |
| Path: | C:\Program Files (x86)\Internet Explorer\iexplore.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1972 CREDAT:17410 /prefetch:2 |
| Imagebase: | 0xe30000 |
| File size: | 822536 bytes |
| MD5 hash: | 071277CC2E3DF41EEEA8013E2AB58D5A |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | low |

### 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