ID: 358592
Cookbook: browseurl.jbs
Time: 22:01:30
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

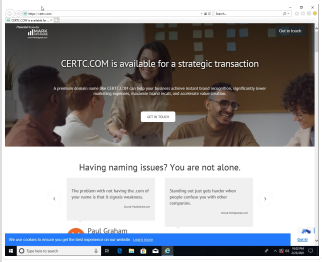
Analysis Report http://certc.com

Overview

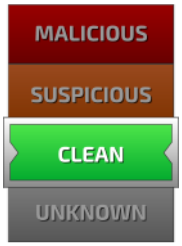
General Information

Sample URL:	http://certc.com
Analysis ID:	358592
Infos:	

Most interesting Screenshot:



Detection

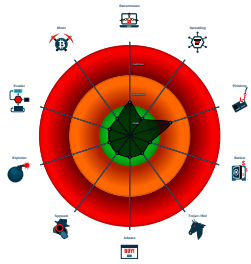


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Found iframes
- HTML body contains low number of ...
- HTML title does not match URL

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 5084 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5188 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5084 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

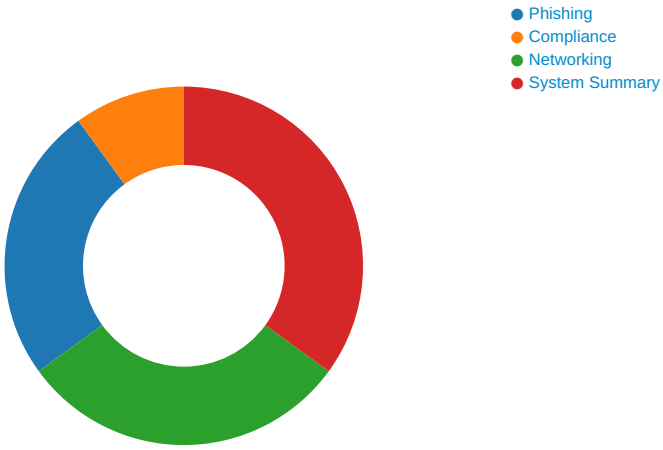
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Compliance:

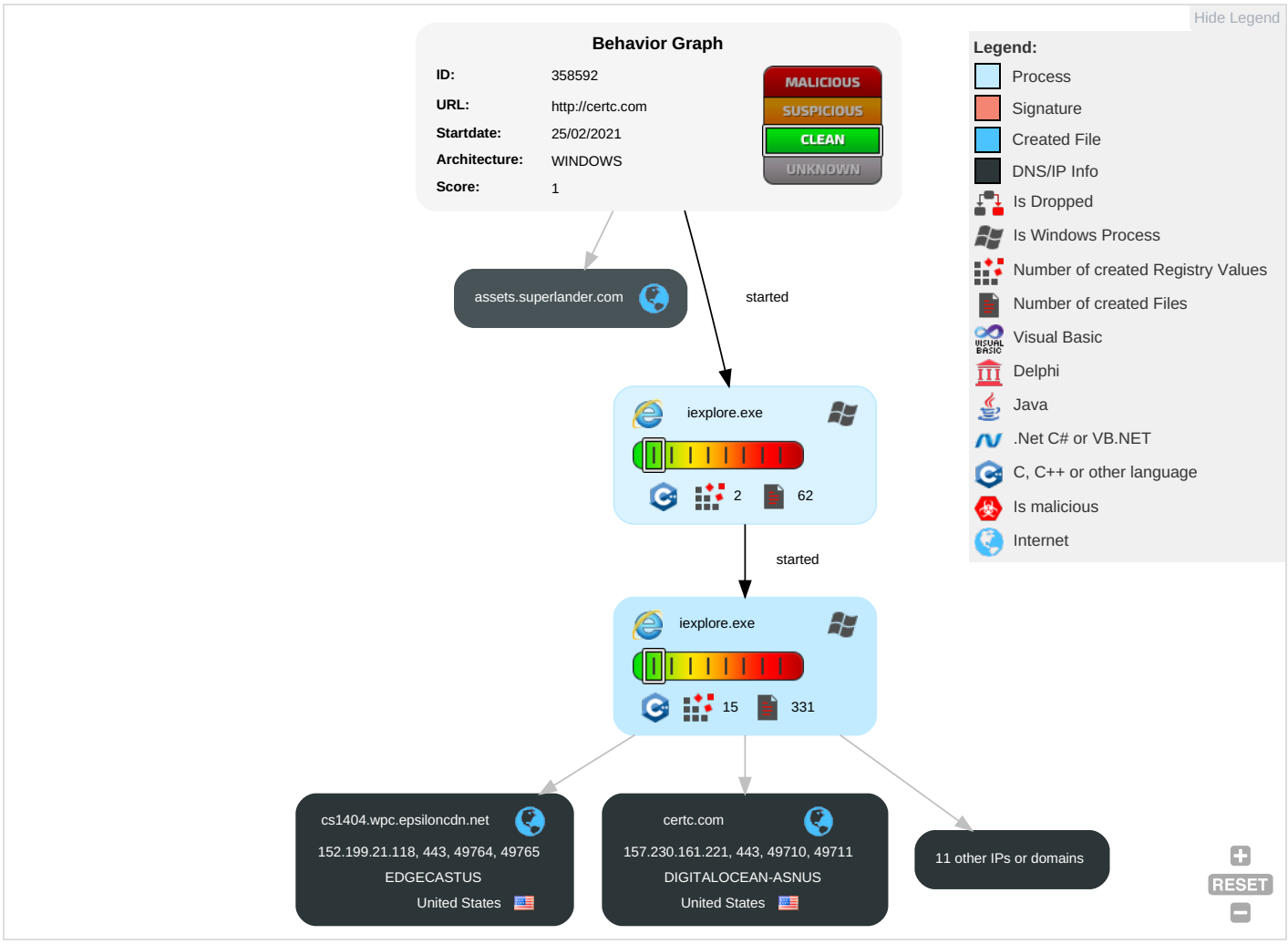
Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

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
Drive-by Compromise 1	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
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 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
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 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap	

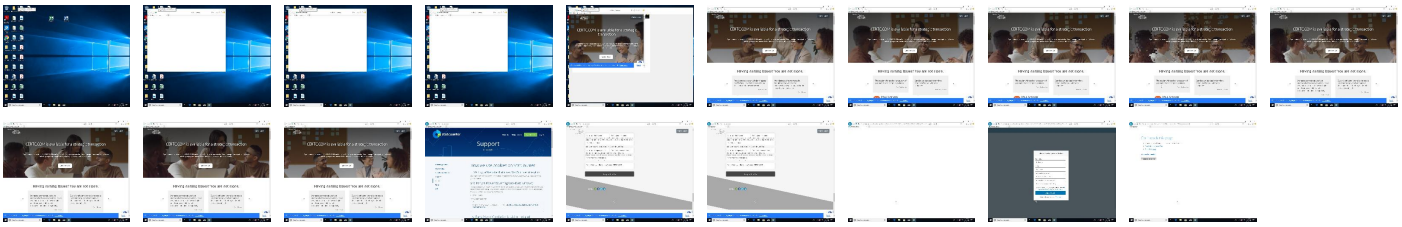
Behavior Graph

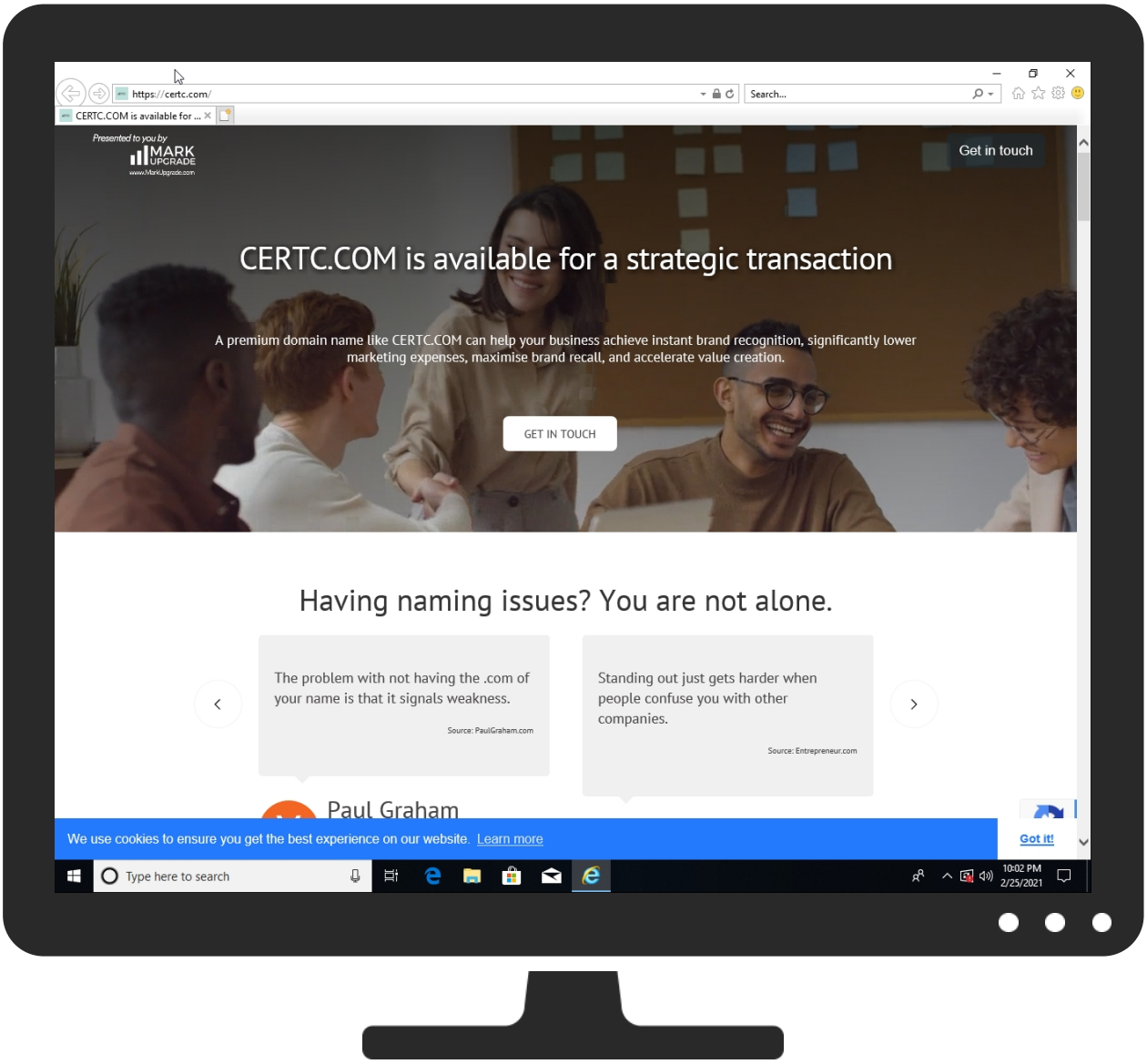


Screenshots

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://certc.com	0%	Virustotal		Browse
http://certc.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://fireworks.abeall.com)	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/jambaimg.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/buttonspic.jpeg	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://assets.superlander.com/images/qslider5.png);	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/Page-8.jpg	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/ebayimg.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/alanimg.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/14-wall.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/clutterimg.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/collab-poster-00001.jpg	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/Photo-10.jpg	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/loontxt.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/favicon-32x32.png	0%	Avira URL Cloud	safe	
http://https://forms.superlander.com/	0%	Avira URL Cloud	safe	
http://https://CERTC.COM&text=Jn	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/Photo-14.jpg	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/Photo-5.jpg	0%	Avira URL Cloud	safe	
http://https://certc.com/#con	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/collab-transcode.webm	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/4-wall.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/blendimg.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/jasondave.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/qslider10.png);	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/css/faqs.webflow.css	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/css/newform.css	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/Photo-3_1.jpg	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/tracy.jpg	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/uberimg.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/19-wall.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/facebookicon.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/Page-4.jpg	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/presentedbywhite.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/tinktxt.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/slackimg.png	0%	Avira URL Cloud	safe	
http://certc.com/	0%	Avira URL Cloud	safe	
http://markupgrade.com/docs/CN_Premium-Domains-Intro.pdf	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/closetxt.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/collab-transcode.mp4	0%	Avira URL Cloud	safe	
http://https://spkt.io/a/616791	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/Photo-1.jpg	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/carrottxt.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/tbsignature.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/fireflytxt.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/TB.jpeg	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/ms-icon-144x144.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/6-wall.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/apple-icon-152x152.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/qwiltxt.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/qslider4.png);	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/flipdish.jpg	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/battle-black-black-and-white-1498958.jpg	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/12-wall.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/peaktxt.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/fortnitetxt.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/favicon-16x16.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/neighborimg.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/casperimg.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/twitterimg.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/apple-icon-120x120.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/tn.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/apple-icon-57x57.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/phraseapp.png	0%	Avira URL Cloud	safe	
http://https://certc.com/Root	0%	Avira URL Cloud	safe	
http://https://CERTC.COtc.com/	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/fbtxt.png	0%	Avira URL Cloud	safe	
http://https://assets.superlander.com/images/17-wall.png	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d1tdp7z6w94jbb.cloudfront.net	13.224.94.23	true	false		high
c.statcounter.com	172.67.38.97	true	false		high
statcounter.com	104.22.53.65	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
assets.superlander.com	172.64.141.10	true	false		unknown
cs1404.wpc.epsiloncdn.net	152.199.21.118	true	false		unknown
www.statcounter.com	172.67.38.97	true	false		high
certc.com	157.230.161.221	true	false		unknown
code.jquery.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
ajax.aspnetcdn.com	unknown	unknown	false		high
static-exp1.licdn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://twitter.com/share?url=https://CERTC.COM&text=Just saw CERTC.COM is available for sale	false		high
http://https://www.facebook.com/sharer.php?u=https://CERTC.COM	false		high
http://certc.com/	false	• Avira URL Cloud: safe	unknown
http://https://certc.com/	false		unknown
http://https://statcounter.com/about/cookies/	false		high
http://https://www.linkedin.com/error_pages/unsupported-browser.html	false		high

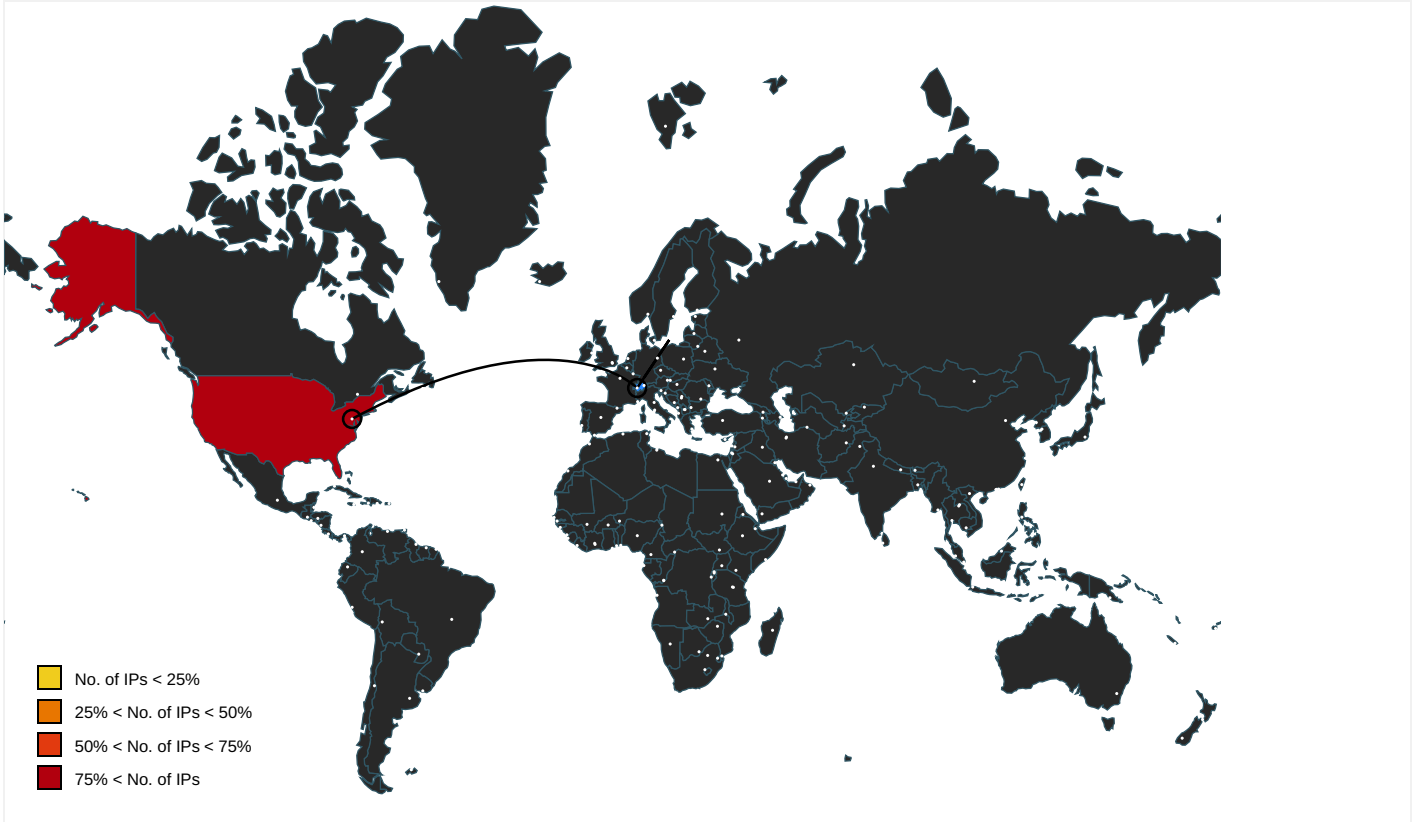
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fireworks.abeall.com)	header_internal_3000_new-13e4be5dd4[1].svg.2.dr	false	• Avira URL Cloud: safe	low
http://openx.com/	cookies[1].htm.2.dr	false		high
http://https://ajax.aspnetcdn.com/ajax/jquery.validate/1.11.1/jquery.validate.min.js	10YYSL0G.htm.2.dr	false		high
http://https://assets.superlander.com/images/jambaimg.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/buttonspic.jpeg	generic-landers.webflow[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/qslider5.png);	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.linkedin.com/in/tatiana-shuvalova-bonneau/	{2B7754B9-77F8-11EB-90E4-ECF4BB862DED}.dat.1.dr, ~DFB705FDC64D3AD8A1.TMP.1.dr, 10YYSL0G.htm.2.dr	false		high
http://https://twitter.com/share?url=https://CERTC.COM&text=Just	~DFB705FDC64D3AD8A1.TMP.1.dr, 10YYSL0G.htm.2.dr	false		high
http://www.rubiconproject.com/privacy-policy	cookies[1].htm.2.dr	false		high
http://https://assets.superlander.com/images/Page-8.jpg	generic-landers.webflow[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/ebayimg.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://underscorejs.org	third-webflow[1].js.2.dr	false		high
http://https://assets.superlander.com/images/alanimg.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/14-wall.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://es.statcounter.com/about/cookies/	cookies[1].htm.2.dr	false		high
http://https://assets.superlander.com/images/clutterimg.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/collab-poster-00001.jpg	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/Photo-10.jpg	generic-landers.webflow[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/loontxt.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/favicon-32x32.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://forms.superlander.com/	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://CERTC.COM&text=Jn	{2B7754B9-77F8-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	low
http://https://assets.superlander.com/images/Photo-14.jpg	generic-landers.webflow[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://webflow.com	third-webflow[1].js.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://bugs.jquery.com/ticket/12282#comment:15	jquery-1.10.2[1].js.2.dr	false		high
http://dev.w3.org/csswg/cssom/#resolved-values	jquery-1.10.2[1].js.2.dr	false		high
http://https://assets.superlander.com/images/Photo-5.jpg	generic-landers.webflow[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://networkadvertising.org/managing/opt_out.asp	cookies[1].htm.2.dr	false		high
http://https://certc.com/#con	{2B7754B9-77F8-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/collab-transcode.webm	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/4-wall.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://pl.statcounter.com/about/cookies/	cookies[1].htm.2.dr	false		high
http://https://assets.superlander.com/images/blendimg.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/jasondave.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/qslider10.png);	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/css/faqs.webflow.css	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://statcounter.com/about/cookies/F	~DFB705FDC64D3AD8A1.TMP.1.dr	false		high
http://https://assets.superlander.com/css/newform.css	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/Photo-3_1.jpg	generic-landers.webflow[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/tracy.jpg	generic-landers.webflow[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/uberimg.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/19-wall.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://bugs.jquery.com/ticket/12359	jquery-1.10.2[1].js.2.dr	false		high
http://https://assets.superlander.com/images/facebookicon.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/Page-4.jpg	generic-landers.webflow[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://d3e54v103j8qbb.cloudfront.net/img/webflow-badge-icon.f67cd735e3.svg	third-webflow[1].js.2.dr	false		high
http://https://assets.superlander.com/images/presentedbywhite.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/tinktxt.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.linkedin.com/error_pages/unsupported-browser.html	{2B7754B9-77F8-11EB-90E4-ECF4BB862DED}.dat.1.dr	false		high
http://https://bugzilla.mozilla.org/show_bug.cgi?id=649285	jquery-1.10.2[1].js.2.dr	false		high
http://https://assets.superlander.com/images/slackimg.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://it.statcounter.com/about/cookies/	cookies[1].htm.2.dr	false		high
http://markupgrade.com/docs/CN_Premium-Domains-Intro.pdf	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/closetxt.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/collab-transcode.mp4	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://fa.statcounter.com/about/cookies/	cookies[1].htm.2.dr	false		high
http://https://spkt.io/a/616791	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/Photo-1.jpg	generic-landers.webflow[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/carrottxt.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/tbsignature.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/fireflytxt.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://statcounter.com/	cookies[1].htm.2.dr	false		high
http://https://assets.superlander.com/images/TB.jpeg	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/ms-icon-144x144.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/6-wall.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/apple-icon-152x152.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/qwiltxt.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/qslider4.png);	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/flipdish.jpg	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/battle-black-black-and-white-1498958.jpg	generic-landers.webflow[1].css.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/12-wall.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/peaktxt.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/fortnitetxt.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/favicon-16x16.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://forum.statcounter.com/	cookies[1].htm.2.dr	false		high
http://https://assets.superlander.com/images/neighborimg.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/casperimg.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://hu.statcounter.com/about/cookies/	cookies[1].htm.2.dr	false		high
http://https://assets.superlander.com/images/twitterimg.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://bugzilla.mozilla.org/show_bug.cgi?id=491668	jquery-1.10.2[1].js.2.dr	false		high
http://https://statcounter.com/images/opt-out_button.gif	cookies[1].htm.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://assets.superlander.com/images/apple-icon-120x120.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/tn.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/apple-icon-57x57.png	imagestore.dat.2.dr, 10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.imagemagick.org	imagestore.dat.2.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/placeholders/3.0.2/placeholders.min.js	10YYSL0G.htm.2.dr	false		high
http://https://gl.statcounter.com/about/cookies/	cookies[1].htm.2.dr	false		high
http://https://assets.superlander.com/images/phraseapp.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://certc.com/Root	{2B7754B9-77F8-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://CERTC.COtc.com/	{2B7754B9-77F8-11EB-90E4-ECF4BB862DED}.dat.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.linkedin.com/authwall?trk=gf&trkInfo=AQGt2Jl7TktB3wAAAXfbAGRgDOsdnfvWfcNSte09JJ15ir515wS	~DFB705FDC64D3AD8A1.TMP.1.dr	false		high
http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-2.1.3.min.js	cookies[1].htm.2.dr	false		high
http://https://assets.superlander.com/images/fbtxt.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://assets.superlander.com/images/17-wall.png	10YYSL0G.htm.2.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
152.199.21.118	unknown	United States		15133	EDGECASTUS	false
157.230.161.221	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
172.64.141.10	unknown	United States		13335	CLOUDFLARENETUS	false
13.224.94.23	unknown	United States		16509	AMAZON-02US	false
104.22.53.65	unknown	United States		13335	CLOUDFLARENETUS	false
172.67.38.97	unknown	United States		13335	CLOUDFLARENETUS	false
104.16.18.94	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358592
Start date:	25.02.2021
Start time:	22:01:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://certc.com
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:	15
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 • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@3/298@13/7
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://statcounter.com/about/cookies/ • Browsing link: https://certc.com/#contact • Browsing link: https://www.linkedin.com/in/tatiana-shuvalova-bonneau/ • Browsing link: https://www.facebook.com/sharer.php?u=https://CERTC.COM • Browsing link: https://twitter.com/share?url=https://CERTC.COM&text=Just saw CERTC.COM is available for sale • Browsing link: https://www.linkedin.com/shareArticle?mini=true&url=https://CERTC.COM

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 104.43.193.48, 104.43.139.144, 104.108.39.131, 216.58.198.42, 40.88.32.150, 209.197.3.24, 152.199.19.160, 216.58.206.36, 151.101.2.109, 151.101.66.109, 151.101.130.109, 151.101.194.109, 13.88.21.125, 216.58.208.170, 216.58.208.163, 216.58.198.3, 152.199.19.161, 184.30.20.56, 13.107.42.14, 205.185.216.42, 205.185.216.10, 51.104.144.132 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, 2-01-2c3e-003d.cdx.cedexis.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, l-0005.l-msedge.net, go.microsoft.com, mscomajax.vo.msecnd.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, dualstack.f3.shared.global.fastly.net, www-linkedin-com.l-0005.l-msedge.net, fonts.googleapis.com, fs.microsoft.com, ajax.googleapis.com, cs22.wpc.v0cdn.net, fonts.gstatic.com, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing network information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtReadFile 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\DOMStore\6I31UWV3\statcounter[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	241
Entropy (8bit):	4.924174995833098
Encrypted:	false
SSDEEP:	6:JFK1rUF49MFGkqqOJSJ5qJlQV0z1rUF49MFGkqqOJSJ5mUGqlQV0zb:JsrULF57OUq3QWrULF57OUjGIQQ
MD5:	E6B43BCDFB74C66A112FC58F3EDE9A7C
SHA1:	A75D061B4FB5323920A29512B14B976FDB2C70D7
SHA-256:	ADB6C01F4F1097E7A076D3DF08CDAE986A4B24C666CDBAC59A6A0C41DA90C7A3
SHA-512:	D055CB3BB8E588BC967AF877FB693F268F570130071392104C0D546EC3485F155470F72BB6CC0118AD67427D801794DC020B87E6B6508B33AB3948618D2CA847
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="sc_medium_source" value="{"d":1614319366}" ltime="16431232" htime="30870533" /></root><root><item name="sc_medium_source" value="{"d":1614319366}" ltime="17051232" htime="30870533" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\6NZGPBUL\www.google[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	112
Entropy (8bit):	4.976623486058718
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsW+pEeAqvI+jdCBw2z9f3ROqSQVSFKb:JFK1rUFy+pEeAqvAw25f3IQVFb
MD5:	702B9730079021C474036D0AB1571A79
SHA1:	0227DE02F23C109A6C15F4F18D17DA7D45B21BE0
SHA-256:	4D7DD3B719CCD58CDBF2B5B1AC258897622125C1F2B1731A19B6DE1E893FABA1
SHA-512:	E6C11C54A055576DE7C5B508D23F3CBDCC256B948037BE7A03DB8846F32A7D4AA255C30FF4E973B27424A126ABB987A74268FB6B043ABD3675CE1A53547AF0EF
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="rc::a" value="MWIxNmYyYTFxMzVtdXU=" ltime="4080368528" htime="30870532" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\BVIC35K4\www.linkedin[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	335
Entropy (8bit):	4.6491187235928795
Encrypted:	false
SSDEEP:	6:JFK1rUFaQAqVnjlQV0z1rUFifqIMD/xjA7og+ItpojlQV0zb:JsrUZlVnJQWrU3IMljcaJQQ
MD5:	5DB47E8343B8BB47DF44E7C0405B3EEE
SHA1:	CEAD7B2120BBEB5F769929C85A473CB332F0CC56
SHA-256:	05F60A31B80E6A84916F61F64DFC47A8F5E3DF488D936DF77B37624583C56EDB
SHA-512:	18A04C52A47D0AEB8AE7FBA7DB4AEADAB04FC33775724FED383AE3CF1426846D8522A3E9A68887C502129D44F99995ABAFE1F0FE31B244842F857FC6B47DF0EB
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\BVIC35K4\www.linkedin[1].xml	
Reputation:	low
Preview:	<root></root><root><item name="v" value="00000000000000000000000000000000000000000000000000000000000000000000000000000000" ltime="86071232" htime="30870533" /></root><root><item name="f" value="AwIHlXRpAQAAImHbUFfTzoZj1Eyqi8fC6QjI9Fmx9REX3bPOsas9PjU3F-c3AX8AAAGLr4YowLkAAAAAAAAAAA==" ltime="86071232" htime="30870533" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DJ0812D1\certc[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	243
Entropy (8bit):	4.957346971760703
Encrypted:	false
SSDEEP:	6:JFK1rUF49MFGkqqOJW5iIQVF1rUF49MFGkqqOJC9slnlQV0zb:JsrULF57O05iIQprULF57Oy2lQQ
MD5:	0E506F0F01FDB44774B1867F2306FE9E
SHA1:	5BCB88878591DC706ED52FF6ECE056209201AEEA
SHA-256:	7030B0EE3A4820122F05B783F0DD3DFA4D599AEE76256744DFF725C8A9176458
SHA-512:	AC1BA781895076E6EEBD9479A4937F181CF29D2C43C67602A2690625422231034B6860D0DF48652190C1EC6598710D2AE40FE2FC1C63B9D1866125C2AB0A5C11
Malicious:	false
Reputation:	low
Preview:	<root></root><root><item name="sc_medium_source" value="{"d":1614319340}" ltime="4049388528" htime="30870532" /></root><root><item name="sc_medium_source" value="{"d":1614319368}" ltime="35991232" htime="30870533" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{2B7754B7-77F8-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8554733369246086
Encrypted:	false
SSDEEP:	48:IwjGcprGtZGwpLlCG/ap8ljGIpclfYGvnZpvlfJGoPqp9lfBGo4Fpmlf1GW5f9lQ:rZZGtTZG23WZxtZ8fZyFMZ/ZtZPfZ9sX
MD5:	6A40E4EDEF5FA096A0ED61EC58A1BD0B
SHA1:	188A4829779BE5E9C433FEC80B0148CB7C14B622
SHA-256:	B86738370BDA6853BA5B98DADD16EEFB44944B00BA37AB9B6A00A57F104B2038
SHA-512:	9012EB7DA8618BE456B6A04FC9242EF2F328B543CDB6501F5BB24E75B16994D8A791F3FEF1D52675A1BEDEB76046875BA2E6A41D40DE79FFA0E256F9A25E050A
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\{2B7754B9-77F8-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	159464
Entropy (8bit):	2.9143115557971804
Encrypted:	false
SSDEEP:	768:M959Q68R1k7PwK4gsl7LFtrl7L2t3FtQ94QCt3+hhOk4f+:WjWRs+
MD5:	79E28A6CAB204D088C7516C26E72A5E9
SHA1:	AC025402C5CC4B6742C2861122873953C791E143
SHA-256:	6121C74A0D37A827C94D413F15FD4F4A32174D94BBB564989FF8BAFDD3326E7E
SHA-512:	5606DBEF367DAEC0117529E0FB153ADEC9C6D313F59A0476EEB3EFEF661B156FF81F22508538594BAB816215B57ECFAFE29EB529A698CE0781AAF9D6F230A0EA
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\{345611D1-77F8-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{345611D1-77F8-11EB-90E4-ECF4BB862DED}.dat	
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5654738439903406
Encrypted:	false
SSDEEP:	48:IwtGcprUZGwpaiG4pQmGrapbSnhGQpKKG7HpR0iTGIpG:rzZUTQS6oBSnbAlT02A
MD5:	061A128587E962D756C68B296E67ADFC
SHA1:	71D47F90522091623DA2C9C3CF0DB594725F765E
SHA-256:	552B1A04E9E043B7C75A653C807D828D60FD0F98C8D221618111BB189F4476EC
SHA-512:	EA43B2B9CF27EE2D733A9017744FD17F24485301146434CD6ECF209254E21A584A5B4CCD939A5D5AFD2287C8EB139C968AADA013420A9D75323B499DA8CC1E4
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	30025
Entropy (8bit):	3.4830316352840827
Encrypted:	false
SSDEEP:	96:46yxYroNdq87kUxItvO1jIFFeLxHp4A/aR7Vc21/////9kki0ihoer+JHZyb51y:Qndq87nxOErLxt27VXkbEH81Z7Y2200
MD5:	0851E162D56C12BAA871045942DAC6F7
SHA1:	3D00D68DBA01DFDF4E84E881989E90D386AE65D9
SHA-256:	C647B8103C9FDB58EF6534B597CDF283FF50F477F213B5201A20A8D0B329DCE9
SHA-512:	6FE97B3BF0B45935076C80BE17FD00AD41AFB9F6C4808C6FC9EF85BEB7A4F4A915E474F29D9BDC838B711B92610B1E441C17FD1FCDB976B233EC628EB47C814
Malicious:	false
Reputation:	low
Preview:	:.h.t.t.p.s.:.//.a.s.s.e.t.s...s.u.p.e.r.l.a.n.d.e.r...c.o.m./.i.m.a.g.e.s./.a.p.p.l.e.-.i.c.o.n.-.5.7.x.5.7...p.n.g.....PNG.....IHDR...9...9.....s.....gAMA.....a.....sRGB..... cHRM..z&.... .....u0...`..:....p..Q<...[PLTE.....`ihr.....y..|.....EGF\ed...t..SXX.....LOO.....V\[x.....jut.....q.~.....t.....r.....GHH^fe...z..cnl.....jvublk...s ..lyx.....nzy.....lxvmzyz..w..lLL.....{.....n{zp}|...s.....aji...jvt...htseon.....OTS`ji.....o}|=<<.....v.....|..dnmkwv...gsq...ius...o}{q.~...q.}>==\{.....~.....J LLLPO.....KNNNRQ...{.....}.....w.....ORR...FGG]ed.....bKGD...W.....pHYs...H...H.F.k>....ID ATH.c`...`...Q...Ldjdfaec`G.....W#.'.7./..#.. ...0....8../...4#..r....+(*)s....khji.....1.....E..

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\mms\4VNT4SS3\collab-transcode[1].dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	3473408
Entropy (8bit):	7.7074937381344615
Encrypted:	false
SSDEEP:	49152:/ifonuxC1uFFXnJZsnQjg1/PpTZMYnw0W6DU38P+Q2OBJCHkN4Wkfp:iol12XJkR1pVnJDU38P+MB8HkN4
MD5:	F1CA677667EB0FBE1BB86CA5E9DACFF6
SHA1:	8633CF7EC7333A44D58CD3EB66D9E9898E7BEBBB
SHA-256:	3D88DF6BE63DBB8AE3D282A8C1BAE735E1E7240F1B101154125087CED0C526D9
SHA-512:	107B4AF5909CD7C8ECDF7F770C3EC074A2E6D084FA1AEB203E61D3F135760CB80A440CEA2B2EE39083B89FE71ADDDED72F705D31B7C4A6CADEAA63F8D47DDF3
Malicious:	false
Reputation:	low
Preview:	.x/.....T..m...*.%.%.....ld>.W....H..8..s=j..gB.{i?..K^d.....<6.....|...d....{..$.I../.K..W..;1.....yR2D.@}x/\|.".U.J.....}Eo.1$.....&H.O.R.....t.2.+...`.+I.y.s_.n&.4...D..*..V...i....E....pC... ...p%' .sR`..8...0I.<5.id.l.....BGE.d....m{..CzA:72.....Zy<.L.].e..T.v.1.-..;.9..<:....YT"Nx.2..o.yy.....<...o..TV.).B..8.jc...@.....Q..l.~...E..UI..|..M....J.YU-.5Y.Q...-).@nH.R."..v`_... L..)k.A9..dD.....V....avS.%..../..*X.....!...`E...W....C...9...x.{J);..I...c...s.[.KiM...T.....X..X.q.#.~qK....G....|._.dS...nKw..>1.M..:..[.....u 0..'..i.m..F.xL..K.x.....;.....4{8*.....:QW*Y.|pB. ..9...J*.ai.l.\...w...!....u...Q]../...s]....&..T[A8.V].Q...x....n.u...d.....{V..V.Y.&.....>fjx!tcy.O..P....W|..l.{....r..^....K..".Z.z.....Z&.....){.LM.t{.....6.2.f...P.=.I{.^f.6E>?...t..nQt....O..... 1...J.l:%>..p... v....Ej3.....>"a.J...{".....Z.=...'}.Q.l...#Na.CecQ.....<...F..=.<.....1..6..L...q.CZ.g..T(r.3..yQ&..7.U._,...6.u8.....,B.e.8}..L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1-wall[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	7250
Entropy (8bit):	7.92328749355968
Encrypted:	false
SSDEEP:	192:OYLFFFpOeT4+vaDOepFdgSZWn4fuDdkKdUzgFVRRwFFFFF9IZ:ZLFFFpl4uaDOTLnQMdtGMyFFFFF9k

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1-wall[1].png	
MD5:	5BB31AED3D5FA405F0D1746CBC1C11C6
SHA1:	7DA04FE2DD9EF5234E8B42117140CF4C8471ECBC
SHA-256:	D7F7AAF23F37197DC7238B4B01855AB79C535499D18E8A757641821112F51247
SHA-512:	7D59F690C8979F091CB2A18CCCD8B98762CBECA86DBC19F5989FDC7C3D4D3A2098458F762B7E795CE47B195FF62DB9D3216CCE347F568DF95323BE15F7E48D D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/1-wall.png
Preview:	.PNG.....IHDR.....<.q.....sRGB.....pHYs.....+.....IDATx..y`.E..?=3..\..&.B .....)......>...*...w=pe_QP_.....". ....B.....d.~...3..<.N..>....._.]%.,#..`tM]....!,.&.a.4A.K ..BX.M...h...@..... .%..!,.&.a.4A.K..BX.M...h...@..... .%..!,.&.a.4A.K..BX.M...h...@..... .%..!,.&.a.4A.K...Ms.m.6.fS.#5..ui.Wb.9..R6rY!ri!.<.... .E.o..)....nj.....nk...wi.....C...v.xM|..Qm..w|...1.m..6.5.wOB..5.l=u.....P.~....].o*._...yY...N.}. .....oF[a...}0.....z.t.`..n.r,?n....$.P..0t-....j.s.[.i.Y./faZ.<.w...w.w.r../xs.:....w.....N..y.(. (.D^..uV..e.BX...p.{.P.u.....\..s1}./.YH.....@.Z,.@.*.n.b....0...]....uW.}.....R2.....:{\q...:G.....P.m.>..|1...(.....".a.i6.....o.<G....>%.w.K<..GD.@Z..J....v.....$5ai~? ..+4...^.`.....N.>.6.%.....)?.~.)n[.I@}....&2 .....3^..b.!..SG.....4.....|..ljW...*L.fb.2..Q...-..9<6.....}y.{..Q.F.p.9*L.....&,..F..c..zb.}..c.Q..}./..5../..U....H.J~..m>o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\10-wall[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	7045
Entropy (8bit):	7.923806762960929
Encrypted:	false
SSDEEP:	192:I42dzrB8ipR/JHusl2ihXH9mwlmK0nCDxWO9qIZ:I4CztfJHusPXd9TyCDxWO9qk
MD5:	091BDF02E9FC82F6BFC85FF4B439B3BF
SHA1:	548D884C4BCCB7C494C79B4FDA6C8F87CBFAB828
SHA-256:	E0568B4F67057A3513D83A918A8AEF23CCFEFBB5B54557A9E5872DC16E258D53
SHA-512:	BECA651A8F6ADE30704DDD1B57283180B06A3D15176662F463D370C09767E21D0DE7325CF0EFF500A928B3755A4E29CDA75F8DD7788CBA00FFAD18FC51FC49 E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/10-wall.png
Preview:	.PNG.....IHDR.....<.q.....sRGB.....pHYs.....+.....IDATx...yx.U...o.....@B.....2.(...(.\.2..#:.....0.AGG.....0,.l.....=...d...U..M...D...|.'.P9u.T..9U....(..p.i... .2.`..... T!.%.B.KP.....,A."X.*D..U.`.....T!.%.B.KP.....,A."X.*D..U.`.....T!.%.B.KP.....,A."X.*D..U.`.....T!.%.B.KP.....,A."X.*D..U.`.....T!.%.B.KP..... ,A."X.*D..U.`.....g.K*h.....Z.....k...../.s....~Lk..G...rcw8.x<?j}5.`]...)(.....v{.....;.<..k|.ag..W...tcw.q.] IW,.%-.+.....->_....3u.....+.....W....=I...j4t.. 9)....k.G..:..C.(.N... {....0GO.....^t?...m..:.W:.]....(.5.wy..z.qi;....q.1,7....Wm.o.5....H..A.G...v..i4._me~.q..T.....Ic...d.c|.v+#n...y.p..).y.E....z..o}....C'.$...D.6....S.....n...CHp .E.NPt.8.$.;8..)..... ....-:..&.....^=.\vr$I.....{...'(0.....^.H.....N..-....w...S..+:...G.Xn...E..S.v...bo.Qjk...0..'i.I.L..j..9~...K+."SU[O.....o?dY...b..>...$"<....$$t....Z..,.....$**....g.G_.u.A...f`.L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\11-wall[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5580
Entropy (8bit):	7.905240781447885
Encrypted:	false
SSDEEP:	96:CYPPPPcFQBApCBHXPASmgF4cP4RE8i4mTD6OrVotJxP0CjgsGUSq7OCe1Ti1OlBk:CzFQ6p2HfASmJcEpOxKH7ORTpnIZ
MD5:	33AF8C897BC3F8E0BB8C05093AEF9FF8
SHA1:	F5485E9E60EF21F25C7A0D825D10E045D78F79CD
SHA-256:	498C33724E5F6D24A1F85B6F3A53EEA07BD89994D27929F42D5B05F98E1921CD
SHA-512:	911CC8F446324B1E43AEAE1879B1E8ED3DF5071D828F079AD56858AFCC7276D997518CEB62A217683D4E979E9B09D68B1AE542B43291F9383121598CACE5C76
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/11-wall.png
Preview:	.PNG.....IHDR.....<.q.....sRGB.....pHYs.....+.....QIDATx..{xT....kB6.....@.F.(-^ZK.T.S.iU.....b....j.../..`?.R.....Gx...mQ..\..b..IB...^.3...]..\...t.?4{.9s.y..o.3....`8.X.]..7 .#.A.F,...X.-...Z0b..`.2h..e....#.A.F,...X.-...Z0b..`.2h..e....#.A.F,...X.-...Z0b..`.2h..e....#.A.F,...X.-...Z0b..`.2h..e....#.A.F,...X.-...Z0b..`.2h..e..... ...U....R*...D.....spV..B.....J),..+.....uT.3)...%.@JyF.r&8.5.. .Gg./....&.....u...^...].j...#...*....I...~..[?.b...'.b...\p.....H@.....p.B..!.(..g.a...Q.X,V...x.<....K..S..o..&...Jn..6...l."... tr...3u...!.]5V.`i...b..=x...c.4.*!X].h...AP."k..u.....K...V.+.....GQ..$&&F.....G)._...j..>....j..m...../...p&.....OI,....U....8..S..".b.....)fB4..z..u.R..?.....T..m..-.....V1.[.;.....Z..Z.B. .^o..1.,.....K.....'.d.(....y...6-..sT....JIm]-w.u'...@.{Ca.v;.....")....ns....#G.....}{....9..8G...@.X..9.o.....x7.V.....a.....RZ6.....7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\13-wall[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	6784
Entropy (8bit):	7.9228875344791545
Encrypted:	false
SSDEEP:	96:chrI9d5wH2K7qSpXv4DeYLyi8UW9jhiQFQ78WiLIGk1ei6fy/ZuAxBP1P0j5PGkk:cyd6HvuStwnLrWxQ/8W9GkTrxbcbIZ
MD5:	4E4BB100BCE528238D2EFF0F15C604FE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\13-wall[1].png	
SHA1:	56ACB6C1126ECCC4A373BF81B1A7B747F9F7290A
SHA-256:	9BD83565440EC50E978CD2222D5FBD259AC58242C4E398BE7232E03FDBB40A5C
SHA-512:	F2D98ED64B034F072A15D61DF26484E2FD08162E40CA17E345AC2D44BADAB9CA3DCEDF12283FFB6055638D750A49A2EB84349541E692831C496A3A3E3897AB7C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/13-wall.png
Preview:	.PNG.....IHDR.....<.q.....sRGB.....pHYs.....+.....IDATx..{xT....>..$.P..;.D).....X.zyl....V.....b....V....-G....A!.P(.PAT."....I..:...L.\gW.....l.....B..2.v@..D.Kc.ZX.[.....4.....-,.-hailA.Kc.ZX.[.....4.....-,.-hailA.Kc.ZX.[.....4.....-,.-hailA.Kc.ZX.[.....4.....-,.-hailA.Kc.ZX.[....._...I(..B..x.A!A..a..7...K)T.c..j.....o.`....).0Jw.....k.2..+...dUX.?}..T.h.u..... \.D ...Z.T..5...S...T.l4*R.B.h.V.^....I.7c..&.....x..+O.~{.F..0....D.Z.>g.97..m.....R....J!}9.....>..#P..7e....*...s..L....N.. ...&.....s....~@`....x..a./.\g_@..o...I.d.:..R.l..lL...K.....spX..2..'.(...p.>.....$.y.23.+..5..R..H-'J..4z.L....HDN.vF.m..`...V..d..Q.~..S..z.....x._..S....}...)3G)=.@X....[F.....(U.].....<RNl...;.v%.....\...Q..3..v..M.{?.s...>.Hd...5.....p.^..... .B.d.B|.o!...b.m.) ..{..p~.....G% .x...7....*.'F...lZ..:.N7.v]....c.T..{w.^.. ...G.<..A.g.nZ...qv

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\15-wall[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	7741
Entropy (8bit):	7.933696799377181
Encrypted:	false
SSDEEP:	192:d9VwO0OG724zEwtKdt9z0XjpP4RkR7DgG8LIZ:rn0y4HUt+Xjh4+R7jCk
MD5:	12927AE07F41BCF814A16C7CF68DC5A9
SHA1:	9F9856532E878D7CD6BFBBFEC76FA0158BF9DCE2
SHA-256:	0A771F94083AB9330496C131718A73F95AAFD18B256555ABECCFB6BB217BDD3B
SHA-512:	72251ED934C8BFBF7F640EB80A274044BADA5941CDD3FA6F1D9B362B38DEE3600C099270001E4A31932A0AA550A44C9E81F2D0C08DFE2E6A203FAD1B3261802
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/15-wall.png
Preview:	.PNG.....IHDR.....<.q.....sRGB.....pHYs.....+.....IDATx..yx.U..^.t..H.[..b..8.0..&"~.....8.. ..,~...eD2.....*.D.....@v..:.....I.A(`..>O.tU.:u..{.%UUU....|.....a.tA.K..BX.]..... @..... .%..!,...a.tA.K..BX.]......@..... .%..!,...a.tA.K..BX.]......@..... .%..!,...a.tA.K..BX.]......@..... .%..!,...a.tA.K..BX.]......@..... .%..!,...a.tA.K..BX.]......@.....pE.....a...v..NpsqE.2...*...G@...e.q...R.o..!....)C.N...p(d.Z.....r..T..$..k*.E_%.h.....<... .....*ZQ<^OE.e..*7.....T..C.r..R..I....@UU.....X.}..".MX..P...}.a6.4a..A.....)..B..-),.cW.iB.....-.....Q.N.tjG..k..e+..p8..aC.i.w-.,rY.9.....0...QT.....t.....C....$I...D.Ym{.G.J....g_...T.x[c..X....7..%.....)++g..iyk.j+^...1..2T..A.b4...mT.c.;.;.s.q.P.6[9.....v.9..?^F...8n..!A..x.r=.....9.w..1.....PJ...j..<B.....%.....x-.9O#.....7q:.y.H.... $8.....#.E.d..(.%..|..6.....,A..Jn.y..8.@...iQC...*...8z*..'..-...R.F.x..kk.6.H....3;'.....JKK..X

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\16-wall[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	9578
Entropy (8bit):	7.940627182530629
Encrypted:	false
SSDEEP:	192:Vg/ImAylDsRgp5dIilKtfPNpywv+OtGv0WavjZXp8qCGAp2WV0vQvTIZ:ugm5DsgpP8hjzvJp8v93Tk
MD5:	53C54821A1F9AEE1DFF9A57B2DC7D2F3
SHA1:	EAAD64FA80F681402DFAAB62EB63F65DDE76D825
SHA-256:	8FF59481F3E3AC53AE65DAAD0985C1C73D834D82CDDE308BC45221B16376B06A
SHA-512:	7643487DAEF9F4C572832713E92B4E5B3B8A710FE3BA3B6E6847C7FF42A0A35412FD03574FA1AFF663A33BC6F5445C7D1D4FF57634D0FAA09ACE5A7F42EE2AE0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/16-wall.png
Preview:	.PNG.....IHDR.....<.q.....sRGB.....pHYs.....+.... .IDATx..y.U...s.]z_.....5 ..w%...2$..1&..f.!j.|.g..$j.....$>...M41a..7. ."(;.....n..w9...?N...%....y.....u....T..U.a.1...gdo.@.g.@.....rB V@N.....X.9!.+ '.b..@.....rB V@N.....X.9!.+ '.b..@.....rB V@N.....X.9!.+ '.b..@.....rB V@N.....vo...b..x.....W3 rP..#l.Vkd8|...4.b..q1;,..0.~..1.%1..O..~H6.Y.....B...H....Y..UX.S\.....a....R..Be2...*.N....L*..f.,..$..1.m...FcK..hK..@H.....G. .A|..().t..F/.M....g.r."..xB.%....Fh0B .A.Xm4..mY(.1n.....!...Axh-y#...TC.....!-....J.....<t.E%....H..Cz....v.zw+nC#^*..F:6Ji0.aYh. ..3..7.Ai.6.)...Md.....m|,.Y..!i....Ey.i.&.D.U.....B....p..X...WE....{.ES&..5.+?....i..V.{...bdcm.x..H..L`..!.....(8.dJ.p.V^./. ..fZ_z...I.....X..I..h.....h@.....1.....GM... /.`F.@..'..m....bI.-@...6...Q~....1.pM..m..[G.s/....][.#S...Gu.@e.Ja\.A.<...ia...X....86vq1..J.cFPx.T\~...].[.@..t<.2..`.z.....R.H)..yx.J...7....b.p*...4.W....(!%

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\19-wall[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5373
Entropy (8bit):	7.870364521638623
Encrypted:	false
SSDEEP:	96:rb6obQlZyd1VZohbf08UdHDZBi2jXfBEE6O9sGkAwVI/x:r0yfQbfFUdC4PQFIZ
MD5:	109BB1F303FE2BE34CA1166E871B7FE1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\19-wall[1].png	
SHA1:	68FD4FF7A89271DB21088B4937176196E26291AC
SHA-256:	DAFBDCD1E43B30CCE54CD1B392A1971D3D641A89F607CDAD7EB0277D35DFAF21
SHA-512:	853243091B96D1311687706648676A5384CA3A03CB6679A7669D3BB995C7619FE936B5EFCFCA540B030403980ACFC219661C95EAD7238703722924018F873ADF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/19-wall.png
Preview:	.PNG.....IHDR.....<.q.....sRGB.....pHYs.....+.....IDATx...{x.....'.pU..-..T<E.B.....*(.P..."GnV}....c..<...V.D.HP.zD...U.r3.T.!.....w...%K...b...Y.l..d....l..R.!.....I.... ..%$,a..KXB.....%$,a..KXB.....%$,a..KXB.....%$,a..KXB.....%$,a..KXB.....%$,a..KXB.....%$,a..KXB.....%$,a..KXB.....%$,a..KXB.....%$,a..KXB.....%$,a...^..*.T.?.h. Y....B...v...uL.....h.Z..l:..J..&..W.MX..N.0v.!.~/.m.1.....]CK..{}....>.'$..)eNf..y.....uP..o...I...TS.....L...95..mq>6....."Cd..^..Y..Ah..|..B.....Nl.....N.....1..C.k47.....p-.....<..''..6... .|.....1.J...G.....A...c*....<....4.O...g....d.Z. .....u.E..'..t.<A...o.j.C.q.....:..*|..@x...p.....`.%,...q....c%.....].....w.K.~.'.!.....y)....{&..3..K.]'.x3..fxg].R.e..?..u..7.....:..X..a5.... u....y_...uG.....3.....%....p/..-.#....=../...1.....U..*@....X..rT.)0...<AT..\.....aT...../.B....o~O.j...9.Z-?.....6..k..h....E.?<.v...P.1.+.~E{..m.P-..B..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\2-wall[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	10593
Entropy (8bit):	7.951936022226464
Encrypted:	false
SSDEEP:	192:0v42LTFBE1IjXIfOCfzMTu6J90CJfV0wyWRfXKXhyL47+XYIZ:0vVjE13Hfiu6JVL0wzsy6k
MD5:	A50CB3300C79B710FE53BA90433439CF
SHA1:	D93FC0C89A4C110A6F59B6CDF3EFED4A1A1A175C
SHA-256:	ACD8CA32664354F596C2C7ABE5D551DFCED2177EC0B7C11265C03E4F84F37333
SHA-512:	3E86C8CCADF749C84210BD202EDD424843E28566DE74BB44C0A3CC6817ACB3CEC660102864070ED164CA483E6F87F52E17568CD87608BDC0ECF92695285FF3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/2-wall.png
Preview:	.PNG.....IHDR.....<.q.....sRGB.....pHYs.....+.... .IDATx..y.....>...f.m``...Q\.....b4n$.....&.&^...1.. .....b\@VE...a.a6f?Kw...s..4.I.....#...S]].....{..!_NBa..B(. .@.....B.!.VH .....PX!...+$.Ba..B(..@.....B.!.VH .....PX!...+$.Ba..B(..@.....B.!.VH .....PX!...+$.Ba..B(..@.....B.!.VH .....PX!...+$.Ba..B(..@.....>+Z.vQZSS..!'...c.....s=.V.Ai..^ ....Z..B.....q.?..<.c....@w2IWW...477#..4J.... .@.bF+....!.....xZ.....h...w.@.3b....RJ..xJ.... ..V.s.....C.....B).%-...yN.u.4h.A..V.ng..f'R...18...?O]....h3.`..h.o.h..A P.CZ.L.Zi...j ...../,Y..;y.Q1...t.Z..+7.h..i.F.07(A+...aC.m..M.hv>e.....N.Y..m...r....1..Vg.:.QZ#.Dy.KJ...f....n:S...S... ..]:.....;..K..L].....UR..K..y....hm...XN...Z..HD....\?.....B.(.F.F.... .knL+m.Z+.....k. Q.....+..BZ.5R).R.....5p?.-..4..BJ<.....~.z....F....o.+e.#.e.....F{.Z.<-.Dc.y.\.L..6.>...4.....r5.c.....9...) .....).?^...5.e..3.(.. ,..!$.m.N...3..t...`!D.s4Z.Ot...D..%.? %

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\21-wall[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	9925
Entropy (8bit):	7.952871509582712
Encrypted:	false
SSDEEP:	192:mptSUlNWNFC1gIEvRoJsSGlgC5Q5wmum5Ic2oaHnkQOtdzGESDFVIZ:kZNWNFCbJrC5ZoSzRkQMVGFVk
MD5:	080B12E830C5A5908B4433763FD10C38
SHA1:	0BDC5B9D7D5A536CED085FEC85E236BD7E2D8ADD
SHA-256:	07C81734789619C8D63768E2BB883630DBB021077CB95D00343FB932238AD869
SHA-512:	33088983AC1C0D73B4A508FB786F119527D9D23B015F54C7C83EC5B75EE0BE62C02EF94538EC8F004FE09B262A23AFA5250075A675F6A87DEFCCC9D1D8AF588
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/21-wall.png
Preview:	.PNG.....IHDR.....<.q.....sRGB.....pHYs.....+.... .IDATx..y.....U.}..V....U.T4(.&..ED.L...D.{L..|n....M..hLnL.,F1....D..W.$ I..Ed.....f.,.U....a4.....D....W.....Zk...'..iW...',., *.K,.....".....,*.K,.....".....,*.K,.....".....,*.K,.....".....,*.K,.....".....,*.K,.....".....,*.K,.....".....,*.K,.....".....,*.K,.....".....,*.K,.....".....,*.K,.....".....<<.....B...5!$.....c..U.`.9z^..F.a..< ..e.B..+zAr{.S."S.!.Kq..7..Z.+...H3..B...."...O.TBk.@".@...T.:..@ ....)e.`!@b....Z..D]..N.[.&.u.G..O .0.....u.....t.\...p\.!.RDm.h...Kw.>....".iJ8 B$.....'.n.....!.6..v.F...;..E...z.0...t .....A.1..1...ak.D..!A#.B.."....X*.H.*.`1...DH...0.V: ....'&.FiCL.vC.....H.A..t$.4u.B.8.....z.....F.....?..?ZE,..p.t<....H .T,!0...f.....gg&.!...pB.MV.Z...../..M....T,...s.ND...ZS, .@Sv.i....e.-.|..o.....W..MH%..L.h.&@)e&R.o.I.I8Z..%u...>..)..4.AHi,.#q...e.\.)C.JH. ..(.J..E..H,b+.X.....!9....2.....HP...4.=}(=..D+.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\3-wall[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	6366
Entropy (8bit):	7.912088194688939
Encrypted:	false
SSDEEP:	96:LX5J3Dm5hFEuRFVtyEanRLZ2L8EQXg+AR3vUG92k8JtPAnQcBzCsa1zGGkAwVI/x:L7Srk7SQXA1v0PsxB/aFWIZ
MD5:	D35B905DC5AA90AFADFDF84AEC094DA9
SHA1:	28F9F07A25A549B60C4284CD7DBCDAEF44856A52
SHA-256:	49769A506260F971DACFD2C491933F61160EC5475C4B616A0D688110391E9E0F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\3-wall[1].png	
SHA-512:	CF306294A133615324CADD0F8A968E5C82681BC989D4E6BE1E41BD63D2804DD279812A800437A856FAAF5B0FEFDE008952EA83FA43E18804B251ED9DD0BFE32 4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/3-wall.png
Preview:	.PNG.....IHDR.....<.q.....sRGB.....pHYs.....+.....cIDATx..{p.E...l6o.....B..7..8....a...)H..H...\.Hy.O..;.g..<.@)A....r..NI.+...W B..l`...s....s.$`..%^....l.t..7.==..M.4$..... ..D.%...K".).D.R,...X.!H.$B.bI. ..A.%...K".).D.R,...X.!H.$B.bI. ..A.%...K".).D.R,...X.!H.$B.bI. ..A.%...K".).D.R,...X.!H.$B.bI. ..A.%...K".).D.R,...X.! H.$B.bI. ..A.%...K".).D.....j....BXX.....&..Ei.{...QYYI]].F....("##..g.Z.....F"##....`0.B.....X...r..t...~.)yyy.\|>....:u*...DGG.(J.O..i....k.b4..x<...[dff...QU..~..?...\.\.\|.UU.0....1.w.y... (TU..k.....(..F~..._..;....*yx....i.....u+./_.....zQ....j.Y.m.HOOg..<..C.....vc...4.M.p...svw4M....7.|....i.z^..<..#.:t(..c.....vTU.`0.i.>..c.....[%...P.4M.....8p....\..~..'..S.....'N0 l.0..K.}[...x..A]].....z.bbbHLL....~.....``...T....t...r.....h.<<(...l.8p./.....r|>.~..~.TU.j..c....9.A..1c.III..fQ...PU..W.R\\...d2.....[.....h4R^^Nnn..Udd$+V..c..l6,..!!!..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\4-wall[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	7335
Entropy (8bit):	7.939857519267599
Encrypted:	false
SSDEEP:	192:1UElKbKLkVlW0A9FZF0G6RK/6SEVfOQ1lZ:xlKbKWlfoAG6RK/6fB51k
MD5:	BB643572132307BF8880BFCDA6CB1B54
SHA1:	2FF3A044DAE642DBF2EBB208D3BB66E9C4D9C31F
SHA-256:	6899373C4D563070F92DC0CD8B5BA4CED29752AD64C1556D87AAF6DC31CBB70F
SHA-512:	AF2DB87C2C30D4BFAB25DF4D68A3BE56B2D1A2BD31D2A5E4C6E8494F107BFC98D0F583FC8E7C23CE0BDC57D78FE441518212AE88109C937F71CFA339CD5E0 A0A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/4-wall.png
Preview:	.PNG.....IHDR.....<.q.....sRGB.....pHYs.....+.....IDATx..yt.U....^.IH .$..... *.....:.#8~~..,8....qCQ\p.....T.#[X.@V./...N/U..!MB.@^..s.s8$U.u.u..VWI.....?1...@. .D.%..!.@..X.M.b.4A.%..!.@..X.M.b.4A.%..!.@..X.M.b.4A.%..!.@..X.M.b.4A.%..!.@..X.M.b.4A.%..!.@..X.M.b.4A.%..!.@..X.M.b.4A.%..! .@..X.M.b.4A.%..!.@..X.M...UT8.z(EU...Q..".*.uz.-a..m.H.H.t.B....\.._6.W..{p...wR.k$.l....!..#.9.W...d....?.....5...[c..G:...k{1|..7..\N5.;....7t.8.]..FD.cM....sj...#.2.....:....lj..?..B BQ..|~.>/J@...z=F...^.$l..i=...|.<...&..;A...X..".....YZKAm#^E./..U.v,...$\..TdI.....,..S~..u.1.^.[.....#Y{.$#.....V...p.H....#'7.....F\l...&..6..p'.$u.i.~.y~8...W.....5....x..1...K. ^.Qw..`T{.....X..m.R.^..u..~..*...$.....*.b.x;.-.....PU..j^_...n...H..d...%44.@ @uU.....;.....j$U.....T..Oy./.....{HO.F.....AN-."cQS..p....9.n..._)B.....V5....J_g/Tw9.Uxv.F.. ..4z .....g..E|.k/.O.....f.d2".-.d.?@..C..<.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\5-wall[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	8046
Entropy (8bit):	7.9391050330340205
Encrypted:	false
SSDEEP:	192:whYLXXXXXojCFOayvt2bgn1L1Kf6fe5cNxvufsvYzj1XXXXUIZ:weLXXXXXoWQa41LBefs8JXXXXUk
MD5:	2C1D1F64E92A4FC66E094A4EF0255277
SHA1:	D11370686DF49A097F1FFF06544A5DA7FFF18882
SHA-256:	36AB2DEF872D05B9EA3336498CFA2F0401B7DB6C23AB0D3FFBB0C625087E0786
SHA-512:	C428E07B8D070F3BE0E95011111F870E833AD80D606CD3727B8C18E233DACACC2FB1E1F7F3D94FD70217C6F33F28C6A14F0C23FB1AFF7AB3FE3F8F6544549CA 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/5-wall.png
Preview:	.PNG.....IHDR.....<.q.....sRGB.....pHYs.....+.....IDATx..yxU..._s.].\.....@ .WD..".R.E...Q..e..E...Vk..W.ZQ....u... ..H.M.D@.K....sor.3.?n.%7..m.Z;.....3w.... gf>3g..RJ..&F...P.0Q.R.....0.%,.)(a)LA.Ka.JX.SP.R.....0.%,.)(a)LA.Ka.JX.SP.R.....0.%,.)(a)LA.Ka.JX.SP.R.....0.%,.)(a)LA.Ka.JX.SP.R.....0.%,.) (a)LA.Ka.JX.SP.R.....0.%,.)X..E.....2.....Ul\R..&h...3V..CG..R.&...{I.....M..K).....TaI@J(.....l,...I..R...a..D....1.....6....B.8/..3RJ.....a.'>>..R.r...?..p8.:t8B....?.a.0.....>n ...3n@..E...H..0....zDb.@C.}/o.0....?....b...;...=Q.....y...!x.e\}u?t]..79..^CB._...*n.RI.....J@=.....ac._W..'..V..a..R.u**./.}..+..#.B....r.yYhra..Q=.[..j...E!A....($...).J...<%.....0d .....A7w..TX..o^n.s.V.E.....<..Nw...}.....b-<.)..q.4#.p.B.Wep..'>.S.?t.VX@N.....oa....,...v.X..ga.@.g..^.....i=.!.Q.g..'....'.v.k..}...dC.m(}.j.....7..R..h..oc...F.....$#R.~... x6..o.E...bm.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\6-wall[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	7393
Entropy (8bit):	7.922528597461888
Encrypted:	false
SSDEEP:	96:0Hg7S2EUl2ddO8iqSlLCFeWKi87pnAeZm+bZBte6Wf6oCVZSVGkAwVI/x:Yg7odOHNFnAeZzxsfF5IZ
MD5:	08B8E209A78B3461270471A1B29F1AE4
SHA1:	067859CB99C8B2A6859B746AFFCC7CC558DCEDCA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\6-wall[1].png	
SHA-256:	A0552A1E407F0AE046F95FD3C397555EE449E1C3B82E4454C52A0223284BFACA
SHA-512:	6DA634C235D8973DE8ADC78BF7CB0B62252152FFE2D1F83070DC246668C0935866D2122A8CD572CD779C4F894A720F4C63E8C3AE56F0E0246FCD3CC137BDC4
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/6-wall.png
Preview:	.PNG.....IHDR.....<.q.....sRGB.....pHYs.....+.....fIDATx..y....U...2.>.3.*....z.j.Q.x%O.,....K./&J.....~.Kb.|.#....D..".....&. ..0{..{w.y..t3...,.....3.U..9]..s~u.T."..H$....+ .j" ....Kb.R,.)H.$. ....Kb.R,.)H.$. ....Kb.R,.)H.$. ....Kb.R,.)H.$. ....Kb.R,.)H.$. ....Kb.R,.)H.$. ....Kb.R,.)H.$. ....Kb.R,.)H.$. .....+.[\|./d*...]vo..b....Zn.....R,....,l6.%/K....\|D#..r...B ....Hw.YT...WB.^...._k...A..SUU....Z.^4.....@(.....kO1xp.%/.....}.K....w.9w..p:...:.....b].B..O..b^.....PZ.E.?RR.g^..^q..p..D....0.s~DZ..FbtDc...A$.....JH.}@,.EU..W.<.. +..`...r.u.b.[.5.<.^...Z5f?0.....Q..i..(....U..+.V.d.....cD.Qb.....8X..6...4GgP|. ..JEyq7.4M%.iO...p.!.Dy@....m.N8.CU.....".@.A .!....uTE..t...=..z.~+.@0....].9r.....@.]7.Z5\N; %....>....[&....`c..^}m.....1....e..c,X....#Q.0x...(...M;.x.>..9.."f.?...::..y{3k...-[.....ic.....UASs{o..._....Y.p.'.[R..W.Z...m..j.....>..O|...a...?.+K.un...6.....dgyih.l.FN.IJd....y...yk

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\7-wall[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5382
Entropy (8bit):	7.891806051733438
Encrypted:	false
SSDEEP:	96:U2R18B333333333332V0xw9jNCvXEpsxRz9dMfdvpcjiukLkjh33ylyvD3R7x/u8:U2Rg333333333332rjNCvEUzmau4h33f
MD5:	02D893D2D3D6E86930EB28E352EB4C8D
SHA1:	D17CCBDC0D101EC098792D8156C51284BC4FD29F
SHA-256:	8B1B5584D0D9A8385DF42EBDE6B756F05567C555AA5B48ABC0800B6CDF6DFEAE
SHA-512:	28B8CBC75B64CB175FA405C5F59FEBDC9D17FC4966BCC53A1CACA49F7E1683EF9C1959D0811CCF1C68A2FB2959FBB0CD512E59B6A87B73FDA4427CD7B3EB 862
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/7-wall.png
Preview:	.PNG.....IHDR.....<.q.....sRGB.....pHYs.....+.....IDATx...kl.....3s...q....;..PHR ...-IK...@.e[.Ei.tU...*.*...E(...[^t..XZR.@k)M.m.B!.=.....}.sf.}q..;>v..'9A....3....f.. <..Zk...Y....I.%..`.#$X....0B.%..`.#$X....0B.%..`.#$X....0B.%..`.#$X....0B.%..`.#$X....0B.%..`.#$X....0B.%..`.#$X....0B.%..` .#$X....0B.%..`.#$X....0B.%..`.#$X....0.w..0%Z...].s...j..D....Vc..k...SY(..l~x}.....#.x.(5<}rZ{.%.0..R.....8.8....yn&l_.`.....8..P..P..e.d.$.. .#.2.E(R.....QJ.fS8....N..5.`).`i.w.%.....B .K..w..i.%.(.8.U...h..}?]m.2.{.L...lJ.y...3.r.R^5...Z..y...w.u.#../x..@8\F....j."...2..Cho.+.h.m1{.Z..X=\|p..d?....j.G".J.I..R.="..,...}A.[.L.W...i....U..)x%.H..p...A:....."..+..f..2XZkR.....W. u...P,..j.W.....0..Jy.\....x.....O....S...R.RJ.M...>Ay.\N.....>-e...@{.zT;.R.....-..V..D....#.y.....\~.W.;V.`.i..$.es.h3=gZ....5...Y...<..S...9...kb...6...x.q.W.....a<.....BkMi.L*... <R.^.....v...)l."...U....spG....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\8-wall[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	5331
Entropy (8bit):	7.881331658083643
Encrypted:	false
SSDEEP:	96:IOZ/PRfh4TqUiq+kVOGn4MkOq0MwFkIRwjEsCeOn+tyhrWkST4t0N6GkAwVl/x:I8RpqUOO130RiEsBO+ErWDTwzIZ
MD5:	BB39B97DA1E96A4A132ECFBFDC5E1D21
SHA1:	08A9A900417D80A2A6574AD94CCE181836836B8C
SHA-256:	E54C1E35C95B29E263D9C51692AE477738CC6CFAFA93259707ACC80452AB2AB7
SHA-512:	0DF332593A1D7D53AABAD205B6CFDD1584F79988CB0A295157F900B0FEC4F2589688285C11CB09431AA2D0B84D9CE52CE0E6B1A128071A524145E56B0F3A2BE
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/8-wall.png
Preview:	.PNG.....IHDR.....<.q.....sRGB.....pHYs.....+.....XIDATx..{p.U.....B.<$F.@.(.. .f]P.Uvk...Gw..X..u]W.(..UwfxL9c..:.....E..G@.W ..3$.....< 1...8..*U.....<.oG i.5...XW.....K0..%.A... b.F...#.X..D,..".`..K0..%.A... b.F...#.X..D,..".`..K0..%.A... b.F...#.X..D,..".`..K0..%.A... b.F...#.X..D,..".`..K0..%.A... b.F...#.X. a...zD,..".`..K0..%.A... b.F...#..h.Z..$)...@c.....a.v.Vl.....w.D..&.N..P..s..N..;...t..P.N...!.-*1...u..4...d...)...5T....o.6..-....];.s.8.t%*#._n6..w.c.!.]..B..PI...gS..9v...).....+pecC c.UZC8.....y.....bX..<:.n.~..... ..&..o..=.`.^..Ca.Po;h.....b...]....u.....yb...^...k&..s.O.....{t"c..|.XhM..,.9|.+5.....R..Y....|...~...9....X..1.v5.j9|..V...../B.I...AY.....D.Q;..... .....k%.q....H._...[.m. ..[..B.k...M...h..W....k.....H..P.m;-kc...XZk..C..;.mK.?...5.f.."...ll.....Vl..|.,,..26.o....{uF%'.....P/..*.?..}.....>.....F...c.f..~.. .....R....A)...:.,.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\9-wall[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	7270
Entropy (8bit):	7.9269425748792335
Encrypted:	false
SSDEEP:	192:ZHoaVOxY0wN7mFAWFYxhUYcJSpQTfoaVJyPOfny1IZ:9VhjAFTFylmSpeQaTyGfkk
MD5:	990AA3EB422D396B3465104A1E144042
SHA1:	80BA26E355D9B5DC1457A5B80D5FCDF6EBA8D566
SHA-256:	9392B4D9401C0BC0DF918DB3B30125C184ADF7E8F5BD4741DBF76FD6F33AEAA0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\9-wall[1].png

SHA-512:	8D33ACA0D507D57CC42157D1FFDAA760BC6EDBF575BEF16BAD4CD616AEFBE8797887C7F56F333CECAC16362D1A8F29BF62C64C745FFC2135CC12EF31C10C29B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/9-wall.png
Preview:	.PNG........IHDR.............<.q.....sRGB.........pHYs..........+......IDATx..{t...?U..d.OI.mlc..`.c^.....X..p.qL`...q......s...r.!{ .&....97...`.5..aa.....1~.?%..d.43.]..G.f$..6-....<3..U.........I.. `....C....+,K$XaY".....VX.H..D...%...,.`.e..+,K$XaY".....VX.H..D...%...,.`.e..+,K$XaY".....VX.H..D...%...,.`.e..+,K$XaY".....nd5._...@ES ..X.u"2.VX.H..D...%...,..]T.~....I..,z.D....I......V_Q.Z-.......V?..+A.8..). UAiVp.!t..$.Ch.....%..=....;.&,[.3..f.^.....Jf:JS."B[w.w..n.;...Q....$....?L.^.e.v....?)...7>..y...y....1....I...o6.I..Xku. D...~....KD.....P.....`h.z.u{.#.d8~.T.......k...9y....e6...+..\..i..~..fH...........<u..;~.'..`W..65nF9./.....60!1./..?9..T.nr(.;.)q+J-.P..*...}.ZE....i...W.../.s.4T.Vlj.hE\..=.{..^.L>....J.5....A.%.) ...%...*..e.#....Va.7...Q~.....x?G..$@........3yh.C.J.V%u..Na.>...G.&...f$..18.O%V=%.t.HX.7...M.h........0.....y...r..'.c..$.O.;t..uC..9.6.;...B..........f.1.T.}.....{....*..........>e.*..]../

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\CharlevoixPro-ExtraBold[1].otf

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	OpenType font data
Category:	downloaded
Size (bytes):	43776
Entropy (8bit):	6.638862911035625
Encrypted:	false
SSDEEP:	768:DRrbg+iJydycz1dwOCM3REnw85OSf9LR0eB9Z5suZz2R:u+7z1daMiw2pfce9W2z2R
MD5:	1C84E57B0C64303EB65ED4DD6992E07B
SHA1:	2EEE610EE192E23FECAB0A81131F331F9595AE47
SHA-256:	12901807A52622D1452F25B528A198A7095D76046BADE5FFA4A432CE54DDC077
SHA-512:	B3D1ECBB7A0E1B37B27D266FE206BDB3158772CA8A8335B231289DF9FC807E32C1D4F75D372590422D8B12E7620B1A841C1B5C18623E1A061EDA3AB1732D160D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/fonts/CharlevoixPro-ExtraBold.otf
Preview:	OTTO.......@CFF >.V.......b.GDEF......s....2GPOS...5..s...6.GSUB............OS/2jb.....d...`cmapP.X........*head.Zs........6hhea.......@...$hmtx.q-N.......4maxp.SP.........name'-.. ....post...2....... ..P..S..........T}q:_.<........................^.................Y.T.:.T.:.T.:.T.:.T.:.T.:.T.:.T.:.T.:.O.:...Y.(.Y.(.Y.(.Y.(.Y.(.Y...Y...{...Y...{.].O.].O.].O.].O.].O.].O.].O.].O.].O .k.Y.G.Y.G.Y.G.Y.G.Y.+.Y.+...D.O.D.O.D. .D...D.M.D...D.".D.!...O.,.Y.,.Y.?.O.?.O.?.O.?.O.?.....Y...Y...Y...Y...Y...Y.h.Y.h.Y.h.Y.h.Y.h.Y.h.Y.~.Y.h.Y...Y...O...Y.. .Y...O...O...O...O...N...N...N...N...N...:...:...:...:...:...Y...Y...Y...Y...Y...Y...Y...Y...Y.n.E.=.;.=.;.=.;.=.;.=.;.=.;.a.D.;.1.;.1.;.1.;.1.;.1...Y...Y...Y...Y...1...1...1...1...1...1...1...1...1...1.k.;. <.&.<.&.<.&.<.&.<.&.`.0...Z.`.0.`.0.;.&.;.&.;.&.;.&.;.&.;.&.;.&.;.&.;.&.;.&...1.n.2.n.2.n.2.n.2.j.0.j.....$.(.F.(.F.(...(...(.<.(...(...(.........;...;...0...0...0...........;.i.0.i.0.i.0.i.0...0.i.0.c.& .c.&.c.&.c.&.c.&.c.&.c.&.y.&

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\KFOlCnqEu92Fr1MmEU9fBBc9[1].ttf

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.Roboto MediumRegularVersion 2.137; 2017Roboto-Me
Category:	downloaded
Size (bytes):	35588
Entropy (8bit):	6.410135551455154
Encrypted:	false
SSDEEP:	768:6yVJgIpAqZsXgDNHOBBPXNOKdhT1N+06XAxGrzmoqpxk0SnuUR:enq805OBBdhT1NP6XAxGryoqp2
MD5:	4D88404F733741EAACFDA2E318840A98
SHA1:	49E0F3D32666AC36205F84AC7457030CA0A9D95F
SHA-256:	B464107219AF95400AF44C949574D9617DE760E100712D4DEC8F51A76C50DDA1
SHA-512:	2E5D3280D5F7E70CA3EA29E7C01F47FEB57FE93FC55FD0EA63641E99E5D699BB4B1F1F686DA25C91BA4F64833F9946070F7546558CBD68249B0D853949FF85C5
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf
Preview:	.... GDEF......{....dGPOS......|<....GSUB7b.....8....OS/2t.#...r....`cmap......st...Lcvt 1..K..y....\fpgm..$...v.....gasp......{.....glyf.'.....,..j.hdmx......r\|....head...r..n....6hhea......q. ...$hmtx..MO..n@....loca\v@z..l(....maxp......l.... name..:...z,....post.m.d..{.... prep...)..x|...S...d...(.............o......9........................EX../... >Y..EX../....>Y......9......9......9......9..... ...9......9......01!!.!.......!.5.!.(.<..6......................}.w...x.^.^..^..............<......9.........EX../... >Y..EX../....>Y.....+X!...Y..../01.#.!.462...."&.~......J.JH.H......9KK97JJ....e...@....... %...EX../...">Y..../..../......./01..#.3..#.3..#...-#...w.}....}.....`...............EX../... >Y..EX../... >Y..EX../....>Y..EX../....>Y......9../.....+X!...Y............./.....+X!...Y..............................01.#. #.#5!.#5!.3.3.3.3.#.3.#.#.3.#...L.L...:...N.N.N.N..:..L.v.:....f....9....`...`....f.8.9...d.-.&...,...*-...9...EX../... >Y..EX../... >Y..EX.#/.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\KFOlCnqEu92Fr1MmYUtfBBc9[1].ttf

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.Roboto BlackRegularVersion 2.137; 2017Roboto-Bla
Category:	downloaded
Size (bytes):	35208
Entropy (8bit):	6.392518822467014
Encrypted:	false
SSDEEP:	768:53Dmu13ucOmpIN22bN8o6Ze0XlGV+uM49pSeCu7XniviDffw6mo/quUR:lD13DjSNz0XlG0uL9YeCu7Xn4iTo9o/4
MD5:	4D99B85FA964307056C1410F78F51439
SHA1:	F8E30A1A61011F1EE42435D7E18BA7E21D4EE894

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\KFOlCnqEu92Fr1MmYUtfBBc9[1].ttf	
SHA-256:	01027695832F4A3850663C9E798EB03EADFD1462D0B76E7C5AC6465D2D77DBD0
SHA-512:	13D93544B16453FE9AC9FC025C3D4320C1C83A2ECA4CD01132CE5C68B12E150BC7D96341F10CBAA2777526CF72B2CA0CD64458B3DF1875A184BBB907C5E3D71
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf
Preview:	..... GDEF.....z\...dGPOS.....z.....GSUB7b.....OS/2ve#...p....`cmap.....r....Lcvt ...=..xX...Zfpgm..#...ud....gasp.....zP....glyf.....,..i~hdmx.....q ....head...R..l....6hh ea.]....p....$hmtx..<...l.....locaK./...j.....maxp.....j.... name..9...x....|post.m.d..z0... prep...C..w ...8...d...(.....P...EX../....>Y..EX../....>Y.....9.....9.....9.....9.....9.....9.....9.....9.....0 1!!.!.....!.5.!.(.<..6.....}.w...x.^.^..^....g.....<.....9.....EX../....>Y..EX../....>Y.....+X!...Y..../01.!.!.462..."&....+.g..k.kk.k.....J__.__.....^.....&.....9...../.....9../. .....01..#.3..#.3.+..._+...v.S.8..S.8.....z..... !..9.....EX../....>Y..EX../....>Y..EX../....>Y..EX../....>Y.....9../.....+X!...Y...../.....+X!...Y.....01.#.#.#5 3.#53.3.3.3.3.!.3.!.#.3.#.d.C.C..,..E.D.E.E...,...C.@.,....f.....`...`.....f.Q.....S.&.Q...-.r.+./..9...EX../....>Y..EX.!/..!.>Y..!...9.....!..9.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\KFOmCnqEu92Fr1Mu4mxP[1].ttf	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	TrueType Font data, 18 tables, 1st "GDEF", 8 names, Microsoft, language 0x409, Copyright 2011 Google Inc. All Rights Reserved.RobotoRegularVersion 2.137; 2017Roboto-Regularht
Category:	downloaded
Size (bytes):	35408
Entropy (8bit):	6.412277939913633
Encrypted:	false
SSDEEP:	768:PX4i+tezjtQYgu30G0xL9nQbuEL7LQo9SBxQbptqKmomjJlvh:PJ2z3G0xpUusLEBKptqNomjV
MD5:	372D0CC3288FE8E97DF49742BAEFCE90
SHA1:	754D9EAA4A009C42E8D6D40C632A1DAD6D44EC21
SHA-256:	466989FD178CA6ED13641893B7003E5D6EC36E42C2A816DEE71F87B775EA097F
SHA-512:	8447BC59795B16877974CD77C52729F6FF08A1E741F68FF445C087ECC09C8C4822B83E8907D156A00BE81CB2C0259081926E758C12B3AEA023AC574E4A6C9885
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf
Preview:	..... GDEF.....{`...dGPOS...h..{.....GSUB7b.....OS/2tq#...q....`cmap.....s....Lcvt +.....yl...Tfpgmw.`...vd....gasp.....{T....glyf.....,..j.hdmx.....r ....head.j.z..m....6hh ea.....q....$hmtx..Vl..m.....loca?.#...k.....maxp.....k.... name.U9...y....tpost.m.d..{4... prep.f....x ...I...d...(.....q.....9.....EX../....>Y..EX../....>Y.....9.....9.....9.. ....9.....9.....9.....01!!.!.....!.5.!.(.<..6.....}.w...x.^.^..^.....{.....0...EX../....>Y..EX../....>Y.....+X!...Y.....901.#.3.462..."&.[....7l88l7.....-==Z;;.....#...../.....9 ../.....01..#.3..#.3...o.....o...x.....w.....EX../....>Y..EX../....>Y..EX../....>Y..EX../....>Y.....9|../.....+X!...Y...../.....+X!...Y.....01.!.#.#5!.!5!.3.!.3.3.# .3.#.#.!.!....P.P...E....R.R..R.R..E..P....E.....f....b....`...`.....f.#.b....n.0.....+.i...EX../....>Y..EX."/..".>Y.."...9.....+X!.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\OpenSans-Light-webfont[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Open Sans Light family
Category:	downloaded
Size (bytes):	19514
Entropy (8bit):	7.9626289574437115
Encrypted:	false
SSDEEP:	384:qjjMPhSj1fICB56ziDqHV7QMsACAl7aNXAJVhJkDQKHU:qYhw1nmFyHXAJlkDQt
MD5:	09E00AA7622ECE30A0F1E06B55F66C2A
SHA1:	3B118F81AC22A995F7CE5FAF2216012B5D217ADB

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\OpenSans-Light-webfont[1].eot	
SHA-256:	83A5C3512B7E56BEF9B0D5451ADF664B070EB3CF6278E69E2CF4FA0B2D2EF379
SHA-512:	B8D560E6750BFD7308648D160DF695DE5FE63CFE67A472E885462D357AFF6FEB9FDC53FCD3ECD2F5845EAC3A00B8D4C6B1AA922C01E9009D3DD878D53E6B974
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://statcounter.com/fonts/OpenSans-Light-webfont.eot?
Preview:	:L..PK.....................,.....LP....[.@(.......... ....I.....................O.p.e.n. .S.a.n.s. .L.i.g.h.t.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .1...1.0.....O.p.e.n. .S.a.n.s. .L.i.g.h.t. .R.e.g.u.l.a.r.. ...BSGP.................I..3..C..(Z....xZW.h[qJ.x"c.r,g,E.&..C..........@.rX...Y..?&.....+.u...LFM.l...SM.P.....+".betT.R..1..U0.:~b...R......B..uM.4&.>.o]nR...%F(E...-*&....FV.........M=` .8pu.i...R.(.Q,K....[).".............h1........b..(..j../...C.p..yCk.."-9..C.4B.+...:.m...Oa..>E).....h........^.v{......T<KY...s,.P.=.,L..t.c..8.L...v.4...J[q.b..7/s_p..d.!.$..Z.L.D.v.K.$...r.u...V. (....E..$>on%nc...024V..._..quK.(I.a.e=n#sF.JO..L..t.4.H..I..k.(...._.G.A..4.w...(...../.+....<+s.......,.Y>..$.K....L.(..s.)4..m..o.^..P.=2..$..b....9....Z....?...=.62(....<.....+..;.zT.....|V...... ..S....N..Wz...i..:..Ne..ui.."...........[T.+.`y_K...-r.Q.@..).K.\"..C.N.:Q.2...9......m.?.;.7.OW..f..........W......X.mk{......J..O..\...2.j.pT_.o....-..n...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\asktxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	27049
Entropy (8bit):	7.6235756743365695
Encrypted:	false
SSDEEP:	768:nvDizgfD4nQZeujBffffffffffffffffffffffffffffAZaqSEx66sm2P7:vRfDvbjqZPFxEn7
MD5:	5729E10A1BBA4C47DC5E0D86D3DEB1F1
SHA1:	458EAB5CFFB7D48C2C3343709E84DAE6B1BA520C
SHA-256:	DF15DAF935B53C7F91019AE214741D02E20405A5A4BC6DBBC4B97AAA5E414678
SHA-512:	590FE7F4D91433734D14753FB1241F91A52121DA578BAD89B0F07C7F8378E37A6015D4F88B9E72820677954206E9371CBACC0854C123337219B4E0C7DD077BAA
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/asktxt.png
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx...w|.U....MB.!.....M...(..J...HS.0".U..Q)"...RD.V.uA.."..'"JY)..{. 5.-............w.M8._..c.`.r..{.=3.K)................A.. ...`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1..... ...@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`. ......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@. ....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bufferimg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	34640
Entropy (8bit):	7.769709161099555
Encrypted:	false
SSDEEP:	768:2uffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffD:2X1sxboOdRj5Z8Mi4mlf4z
MD5:	4456C428AE7AD71CCCE2948057707DB3
SHA1:	17CBB716935B5EF20E65D7FF420DB748E7538BB1
SHA-256:	343C8EAF5D6DB53DC66254FA48F0C8E2721BB1D718182C66625951E41E630445
SHA-512:	A621464C7BD57DD1B5CF8FBA7AFB85D697D33417A2F2E3DA15B32B06C997CD0225B93DEDB5FB89B85AD9793880DB818AE5024A6867EF88E8C753BFE598BA485E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/bufferimg.png
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx...iS[g...KB...;.}.1.oI..t.;U3]==...S.y1.=...xc..;..&....y.:...l....._U*....h9...L&.........]............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0........... ..c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0. ....c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .. ...!.....0.............

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\buffertxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	22345
Entropy (8bit):	7.483524384430783
Encrypted:	false
SSDEEP:	384:FrWtIghNCZynsHYM2EzbHMOey9VwfffffffffffffffffffffffffffffgRY7pMbcB:FJgTCZynsHYWbHVey9Cfffffffffff5
MD5:	2321AFECDBE4388937ECE97C4DD531E4
SHA1:	DFB9613A35E20156138B1D5C783C174D7DA74FA4
SHA-256:	78D78137EDE4758ADE7A8D976E645A7D0C29AB5A2EF680190EE55F2D6D64C726

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\buffertxt[1].png	
SHA-512:	A9B2EAE6BFE56F18E5EAFE83EB362E4C05A9E9A125BF03C12D0C66D90F19D948F623C89C7BC85009032E02E42369D1429DEDF90D476E09133052BDF2EE41A5E 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/buffertxt.png
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx...wt.U....&..:.....E@D.HGP...B..P|...`E...."...<h.X(.""..*.4..`..zH!e~....0......~...s..-.Ip?;s.uY.e...............|.@..... C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1.. ......@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.... .`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1....... .@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\casperimg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	35361
Entropy (8bit):	7.804974885533988
Encrypted:	false
SSDEEP:	768:aWVOGjR3QYy4TZFmPLR6lxN8c/bs0/IUB3B1l/VvSoo5WMSppppSt2f:NVO0AATmYl0c9/PHlN3cWF
MD5:	DEF41FB61DC61F3B98F3244D09345327
SHA1:	814D9FE07D1821162A2D65C18156ADAD8D10348C
SHA-256:	197CA8EC503116F12D570CF05759CBDCA9ECEA23451BECF348E15E8F28BFFA63
SHA-512:	BAB81430DA75C60D15A0514F144DA21B1BE3A96697FE3E33F681581B8E40CA586521A9EE858E552E3E874644829338BB7C34234EB5981E194E7F8D0B92792958
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/casperimg.png
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx...w.T.....9.N...AA.`..5..Kl1&..Mb....h.7.5.&~.....{.&..v.5VD,."E....Y.}w...........gg.....a...{..9.S>.DQ........]}.....6... ......@....8C.............3........@....8C.............3........@....8C.............3........@....8C.............3........@....8C.............3........@....8C.............3........@....8C.............3........@....8C.... ....3........@....8C.............3........@....8C.............3........@....8C.............3........@....8C.............3........@....8C.............3........@....8C.............3........@....8C.............3....... .@....8C.............3........@....8C.............3........@....8C.............3........@....8C.............3........@....8C.............3........@....8C.............3........@....8C.............3........@....8C......... ....3........@....8C.............3........@....8C.............3........@....8C.............3........@....8C.............3........@....8C.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\caspertxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	29714
Entropy (8bit):	7.547524558105773
Encrypted:	false
SSDEEP:	768:6ffffffffffffffffffffffffffffffffffffffffffffffffffffffffw:9L98cQL6bRlCDiM2p
MD5:	0CADA6D816AF0C5454FB5FCDC5DAB0BA
SHA1:	64742C9237EC08546C1D4E6E4EE0893D5FE293C3
SHA-256:	2ACD5BF35D29C15614E3F62DB637610D38373172DE2C58707C3E63BE031A4394
SHA-512:	8DAE9296F9941F44F7E93077507B5B799B14C2C8D2033253D6D87EED1282884DEB55C2E98AE9DED5038187B57AF3655E9997072F98B4EF0C1C1178D1B79F228B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/caspertxt.png
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx...wx.e...w.I....$$..DD....@h.D.A.a.t.V...GEQW].R...Qa.e.J/......M..@B......?...s..Ay>.k.K......s.5s..?.......0... W....................c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0........... ...c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0 ....c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. . ....!.....0.............c. .....!.....0.............c.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\closeimg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	62157
Entropy (8bit):	7.930617403054332
Encrypted:	false
SSDEEP:	1536:LBc8XF/ekBiyDU5ZoKjQXRG4EzrPjSS7HAYW8:a8XxnDqZoWQXRO7jf7HAYW8
MD5:	148D380C38FD39D09738FB56C98DDE0C
SHA1:	A9405B729755ED615D8F4BC4649EAC63AAB7F57E
SHA-256:	FCE0722954DAAFB1B4BD311CD4EC56659F063E7ED768AF3D264679E643F0A9A2
SHA-512:	18E44AA262B06705EADC274926A8B04083A888CDD501E237BC05CDD578FA6A65E3E198DA9EB7FE2C56DB6E37563D8283ED590FF1051BD922E57FDB953ABE12 DB

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\closeimg[1].png	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/closeimg.png
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx....w.......9...%...`I....3.....93...u.e+X..(...r........H.....||(....M.............}......>.......!@....$............@b.......!@.... $............@b.......!@....$............@b.......!@....$............@b.......!@....$............@b.......!@....$............@b.......!@....$............@b.......!@....$............@b.......!@....$..... ....@b.......!@....$............@b.......!@....$............@b.......!@....$............@b.......!@....$............@b.......!@....$............@b.......!@....$............@b.......!@....$............ @b.......!@....$............@b.......!@....$............@b.......!@....$............@b.......!@....$............@b.......!@....$............@b.......!@....$............@b.......!@....$............@b..... ..!@....$............@b.......!@....$............@b.......!@....$............@b.......!@....$............@b.......!@....$............@b.......!@.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\closetxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	23738
Entropy (8bit):	7.570878293279057
Encrypted:	false
SSDEEP:	384:uDQ58eByer2ZyNFj6pY7HzCtSqlBh+uciCxOvGOk:uD+ByeNcYhqnghXxOed
MD5:	00BF68BA76A0206217BF33B0CD2F1FF1
SHA1:	20E9669B98BAB0AF78A8760ED7C9476C02EC23B7
SHA-256:	F4089516977C332E89B905EF1237BCC8405078C380F04CB16EE9E05E513180DB
SHA-512:	85E2BDC82DB4A6C91F3FF0EFDEB3D5271649B129DADF3BA26612430DF8BBCCF8F4F7AA5D7FFF29EE2948D900914FF1B8FE76F06F81AC1F4451C65CAC6D969 32
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/closetxt.png
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx...yxM....w.!.c.2..1EUc.1..J............h...1..QJ....A.c.E......H"AD.....~.Z{gO.cx>.k_.z.u.k.-Y...^.M)......4p/... ...xp.@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.... ....6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6...... .@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC......... ....6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC............

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\counter_test[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	39159
Entropy (8bit):	5.450542019923853
Encrypted:	false
SSDEEP:	768:dhstO8lVCA45/zUVdlcb6ddbt8utYKmypUX8f/5DB1YSMv13ROXqWiQRKt33JDYE:t8HdjljYZDYXFXUHDlf
MD5:	4DA07DBD600A063A57AEAD6EFF67D2C8
SHA1:	F47EF75ED972F3CFF7742D07D3AFACC47BABB8A7
SHA-256:	C5086D4F97BC3EE70971C51E89FA6AE25FF054ACCEC7C4E890B1083EE7BCC9AB
SHA-512:	4E77F636AA87FD3AF056D1CBCB3FF112981E347D44BB4CD1BF6660CC216835503EAD6EC77A99041CEAC602F92E16136711B9D5CDACFE29AA3E3444853DD0B6 9
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://statcounter.com/counter/counter_test.js?cb=830817
Preview:	var _statcounter=function(_1){var _2=false;function is_admin_project(_3){return [12225189,11548023,11878871,12214659,981359,9560334,6709687,9879613,41 24138,204609,10776808,11601825].indexOf(_3)!==-1}try{var _4;var _5=1;if(typeof _1!=="undefined"&&_1.record_pageview){_4=_1;_5=_4._get_script_num()+1}else{if(typ eof _1==="undefined"){_4=function(){};_4._pending_tags={}}else{if(_1.start_recording){_4=_1;if(_1._pageview_tags_in){_1=_1._pageview_tags_in}}else{_4=function() {}}if(Object.prototype.toString.call(_1)==="[object Array]"){_4._pending_tags=_1}else{_4._pending_tags={}}}_4._session_increment_calculated={};_4._returning_values= {};_4._security_codes={}}_4.push=function(_6){_4._pending_tags=[_6]};var _7=true;var _8=false;if(typeof performance!=="undefined"){try{_8=Math.round(perform ance.now())}catch(ex){_8=false}}var _9=false;if(document.currentScript&&document.currentScript.src&&document.currentScript.src.indexOf("statcounter.com")!==-1){ _9=document.currentScript.src}var _a=-1;var _b="";

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dnserror[1]	
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Reputation:	low
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. <div id="contentContainer" class="mainContent">.. <div id="mainTitle" class="title">Can’t reach this page</div>.. <div class="taskSection" id="taskSection">.. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dollyimg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	30709
Entropy (8bit):	7.63518164645966
Encrypted:	false
SSDEEP:	768:iffffffffffdCeFfffE50MTmo0zA2JG/sd+3846peyy6CDQdKQuVVkQ2fffffff2:p50MTme2JG/sd+XCeyySwJ8I
MD5:	E30FD07429BE99D4F8CB829BA534DE70
SHA1:	09A1DC17902C641FC1089C8ADC0FFA085630290F
SHA-256:	C892B2F8929D958B5D693C51ECE5116D74C24AB730E3AB85C3E31B86386449F5
SHA-512:	53D6755CD7C27C06CE31B532D77C1D5120BC39B482839F1DBF5698E362BB00D7B7A538E480E5D58A352729D29907D48AD683A58074CD1939423F33CA2EC1870
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/dollyimg.png
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx....w.G...'..}....II.%y..U]U==g.s.....O..v.%k.HQ......2/..@."..AJ.~|XV...@&.x"~.a.A................q.@.....C.....` .......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@ .....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1....... .@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`... ....1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dropboximg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	37831
Entropy (8bit):	7.796971717074937
Encrypted:	false
SSDEEP:	768:4fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff6:4JSl4t6Lxioxw/GeWBv38hgwRqcPO
MD5:	FF234361283E082C090D6261440D753E
SHA1:	213F482CC80FB7E45E066C4D0C38DFE7075EC253
SHA-256:	F77740904E867AD2B633FDB7EC31E5AB500B2961FA739260DCEAC0B9F1ACF595
SHA-512:	01C6BDBE22AD19029945E50EDDE93FC317FAA7D8D6BAAF2A74D37375CAF40DB71A00B74F018A9B098B0C1829E8D029D78ABAD9F9D5A39CD8276A34C000AEA8BF
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/dropboximg.png
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx...ip..}.....HB.. ..}....6.q..Y|.q.L.i&....>...v..'M.&.R.....m.b.H,..!.......t.....X..h.$..5..G..:.....Z.6..........0........ .....0.. ....c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. ... ..!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0......... .....c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.... .0.............c. .....!.....0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dropboxtxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	28532
Entropy (8bit):	7.646934973819865
Encrypted:	false
SSDEEP:	768:eZ6yO5SU7i2pA6jdsbftfffffffffffffffffffffffffffffrhwe+nzkx:eZ6hSgi2pD2hV+4x
MD5:	CBC8AF9E80E6A9BD1F07830E35ACFC76
SHA1:	DECF5C35AABE0143B752CD94F5DC91280FF82777
SHA-256:	19622823E955DB298E286E7EDECF54F80FE76FF0A83491983FD010108E8E5A56
SHA-512:	240FAA8DC3AB39C512F9C7C319BD1DE3E73C1B0979F4AECDA592A516808A1B967DD54C1150E2DDEE3B8B1A9F961E201C5796EAE506DCF4D885C49F993C9B79A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dropboxtxt[1].png	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/dropboxtxt.png
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx...wx.U....MBH...B .".R...PB/.. ".......Q.*6.EWAD..... ..JWiJ/B...HMB.......=s........<.G&s..e>3gf\J)%.. ..`@@aw....._.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.... ...1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.... .C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1. .......@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dropimg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	40874
Entropy (8bit):	7.838028937392131
Encrypted:	false
SSDEEP:	768:UjNXF3D1cH3mugoRUSAvNPLhFOucsygx24fe+O7lLL1KTqzWdnrx:UjdQW5/S+mZsyI2Zd5bzGx
MD5:	2239D0AC5466729E02FE900AF2723AE3
SHA1:	300A448BDE7F866DD68DB9680A08F71E3BB75638
SHA-256:	04B0D38D9D197BC8BA1149A8C1215947E2CE0CEC6C054B9C5D72D3D61D44D189
SHA-512:	E8663943BEED62C8EE9C66CEBC44FF33D338A7EEC667C9AE778640CC77DD85F70336CC758A900413C22C575ED0622682B96766CC40F2E1C13035EBFBE99F61 E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/dropimg.png
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx....s....O.f4...}..!....1..&v.....rU.?.?.?me.v.6q.oe..6.`.....@ ..>F3... ..i...<......9zz..~>..m........vo.............1.... ....@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....` .......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@ .....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1....... .@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\droptxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	26818
Entropy (8bit):	7.613975917117477
Encrypted:	false
SSDEEP:	768:iffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffC:xtJhzVqJROCvDHaLDC8
MD5:	782341B2C7106DF3F7871B618DC7B831
SHA1:	042D45A0D95BDA9A79DBC258EF32997CCF68FF23
SHA-256:	D191D5BCAFFCCEC044B1F22D83EA8D19E6176DFEB30BC94FADC22BEBA477B8E4
SHA-512:	8450C390EF9D0085005568F9452349D36080C21E9258019C0C5D116907269E4B91C904930A28105C108ACCAF50A681DF7B6593A8326FEDFFB103C92EBED0A8B0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/droptxt.png
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx...y\U.....aP.Y...QDK.9O.C.C.WEm0+.Qf*....5....).n...y@.f*.)N.!....~...oz.....z>.....k8.s...^{[.RJ.......;=....... ......c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!... ..0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.... ....c. .....!.....0.............c. .....!.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ebaytxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	27345
Entropy (8bit):	7.591002424018381
Encrypted:	false
SSDEEP:	768:Uffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffy:oHBDv98DHi1wDcoqkeXV8J
MD5:	0D1D06592643A8CE000716D2114D4870
SHA1:	D0196CDBDEFC0E337C88EB0AB9639C876EDAAE5A
SHA-256:	9E7E1FD235BB20B43656198361CA2CD5EDE7B12107098FF6CC77CD1832D54D6C
SHA-512:	835570FA32B24565067C02467611C6BB7E00D075035FD24D60E4948B7D49D2436A0936D14126F60DF6F8B0F1C0EA56E4780DE8A5F0432B0D7B687DCE7C6045F4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ebaytxt[1].png	
IE Cache URL:	http://https://assets.superlander.com/images/ebaytxt.png
Preview:	.PNG.....IHDR... ... .p.h....sRGB.....pHYs.....+.... .IDATx...gx.U...o.I ` ....."`....QDXWp..b....(.*.....- . U. MZ..P.$.....'.{r..~].<..s..e2..93^J)%....`.w~w..... .....c. ....!.....0.....c. ....!.....0.....c. ....!.....0.....c. ....!.....0.....c. ....!.....0.....c. ....!.....0.....c. ....!.....0.....c. ....!... .0.....c. ....!.....0.....c. ....!.....0.....c. ....!.....0.....c. ....!.....0.....c. ....!.....0.....c. ....!.....0.....c. ....!.....0.....c. ....!.....0.....c. ....!.....0.....c. ....!.....0.....c. ....!.....0.....c. ....!.....0.....c. ....!.....0.....c. ....!.....0.....c. ....!.....0.....c. ....!.....0..... .....c. ....!.....0.....c. .....!.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\email[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 64 x 64, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2820
Entropy (8bit):	7.922954660850759
Encrypted:	false
SSDEEP:	48:IL5bN3XuVQ8/lqHanXCEddzkOvtlsHEVFbuw4e0sOeT7y8c7P+iSLm+nC5eBdDs:AxN3XuVHNq0XXd45HEXdfNGZ7FSNn3dw
MD5:	420C63238AB1E9BC848AF40DEAE4CE23
SHA1:	A9150948EFD42D0EF9D5BC12BCBDD3C83D4F4073
SHA-256:	F72A9160A05E60EEC1A99CFA47559CD53B939CA4E171194CB227C9E8E891E17C
SHA-512:	B8FF3AC5E54764A5B1E3874A469BC7AD25C85006F015F77477052457DC6864A3A751DC37F069AE507F0CE268C297F1959F5E34B12BDD3B69B4CB7C334033C438
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/email.png
Preview:	.PNG.....IHDR...@...@.....iq.....sBIT....|.d..._zTXtRaw profile type APP1.....JO.K-.LV((.O..I.R..c...K.K.D.....04006..F@.9T(.....Y..)....O..h.-....PIDATx..ypU...?.{.[.6Y ..B..."1..*...AAJe.[eI.Ih..SG..3.t..t...I.."..VT@.B.A...AB ..Z...^...AB...%.=,...=.....+D..E#o5.F..$.....t...Jk..Q.R8)B..GT(5U.../...2..$.F3.G'a..Q.B$E.[.2.zN...kl.....cGRk..0..{....O. H....#R...UT.#.g:..9k.H.m..f/...T+C.x.!1....Z.h.....x...-1.....\8*..Y.....K. .{M..%.....?]:.6.....L..}.Q.bKz....P....cDt. w..6..)..E...2C...3.i...g.."....L.el_qxC.....j.-5^.x*l}..>..d../.....Y..8 .h.DD.....).fl..\=#.%..+.o...aL|m..@....2sG?%...-..R&.tm_qx]3u.fNN.(.Y....bzvF..M.4....0.K..Q..3.=....hN~.....-.f.i,.Y.. .-..;O.....e.8...S...c#-v.2..%...z#f.....+..^...C.o..$.....Uw@. .y...@h..?...zf/....{....[m.....0]....u.(z.g.....x..j(.l.....6..... ..*R.#B...w9..z'4. m,....A.....8.d.Z.....I..\..s..u...3....[...j...kj_.{.u`..*.....c`.....8-w..".K.6.A...&.....,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\faqs.webflow[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	4142
Entropy (8bit):	4.84485449913067
Encrypted:	false
SSDEEP:	96:Nrux7NOJFtjnzzCfdAiTeIpFakFwu5uQEC80BCv9wMjib4g/ji4NtFjmh9k6g5Fh:gNuFtjnzuGGFFvFpoFzje4g/jDLFjmhK
MD5:	CD3E87556B1F43E1858EF2321C5EFD16
SHA1:	174D9949C945F8094B16B41AA2F1368CD40D5BE5
SHA-256:	062DE81F59553587FF396B47FC62B4B4AF55FD6F7FE0DC42F19A066046371CB6
SHA-512:	A444E2F2E3EBE680E6396BF28B4BC962617AA81002C5763F2CC5E1A4CCBD9A6932AC511BD7FCF67FD0F748E2994E9406AFB763E61BE8B9CD696414B73437AB3 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/css/faqs.webflow.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\faqs.webflow[1].css	
Preview:	.faq-q-text {. margin-top: 0px;. color: #221f1f;. font-size: 20px;. line-height: 1.5em;. font-weight: 600;. text-align: left;.}...h-div {. width: 50px;. height: 2px;. border-radius: 100px;. background-color: #583bb5;.}...container-6 {. position: relative;. z-index: 2;. display: block;. width: 100%;. max-width: 1400px;. margin-right: auto;. m argin-left: auto;. padding-right: 5vw;. padding-left: 5vw;.}...container-6.faq-container {. max-width: 80%;. padding-top: 60px;. padding-bottom: 40px;. border-radius: 5px;. background-color: #fff;. box-shadow: 0 0 50px 0 rgba(45, 62, 80, 0.06);.}...faq-answer-2 {. overflow: hidden;. margin-bottom: 12px;. padding-left: 45px;. border-bottom: 1px solid rgba(193, 191, 189, 0.4);. color: #221f1f;.}...faq-question {. display: -webkit-box;. display: -webkit-flex;. display: -ms-flexbox;. display: flex;. height: auto;. margin-top: 20px;. margin-bottom: 0px;. padding-bottom: 20px;. -webkit-box-align: center;. -webkit-al

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fireflyimg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	106096
Entropy (8bit):	7.967861215012008
Encrypted:	false
SSDEEP:	3072:DItRNo1jDiiYsG53wZL0qaObqYkayyGsyblSxJ:DItM1XiDszS9JyryQr
MD5:	EC4AFF984FF12F1AE89709AB66913D2E
SHA1:	89B141A8DAB15CA3C0BE1756A40D86EF1ED22AD6
SHA-256:	308D6EEB8F14C3DE0CFB96996DB21F24EE5CE86D893E6FD82E97824D24129A07
SHA-512:	8555ECE35AA6503ECBC2D537794A7D827F15278EB8B60A59DC5E41BF2C18AFE35AA8B821A9525E8D911FD426317329F1036780E55642DCF72B3840A04E3EAC2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/fireflyimg.png
Preview:	.PNG.....IHDR... ... .p.h....sRGB.....pHYs.....+.... .IDATx....$.Y.....U{.M-.%.,0.....I/.....f.a...`,Y...{}..2#..""2...d!.....k.%+.I.O<.....X@.....`1.....!.....X.....b. .....C.....@...,.....`1.....!.....X.....b. .....C.....@...,.....`1.....!.....X.....b. .....C.....@...,.....`1.....!.....X.....b. .....C.....@...,.....`1.....!.....X.....b. .....C.....@...,.....`1.....!.....X.....b. .....C.....@...,.....`1.....!.....X.....b. .....C.....@...,.....`1.....!.....X.....b. .....C.....@...,.....`1.....!.....X.....b. .....C.....@...,.....`1.....!.....X.....b. .....C.....@...,.....`1.....!.....X.....b. ...C.....@...,.....`1.....!.....X.....b. .....C.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fireflytxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	26355
Entropy (8bit):	7.603147312160931
Encrypted:	false
SSDEEP:	384:9Q78qD9qzDwatmGFkzyhNdpoXqZ/CdXX0SJVfjuJO09CLYpV+ToCX8k:U8qszh7hhN7oS/Cd9teOZpoCj
MD5:	9202CBCB9E63F81C57C8F1947F24EE4F
SHA1:	3F29D5B9527E552229B86BBFC7562319E2D89DF7
SHA-256:	C38C094C8BAEAC3B228C3B74B368846930F377BA6D1FCFE654970DFDB4BB00A6
SHA-512:	7773D29A45E09696D6DD68DA0C37340ED0C557FF8090826A3699C67164A2E36CD01325ADAD1394C55B773D5DBC29ADE6ECD1806AA8E339FF6825F7AD59265A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/fireflytxt.png
Preview:	.PNG.....IHDR... ... .p.h....sRGB.....pHYs.....+.... .IDATx...y.Ou....,1...Y....]...,..I.*\....*#B.5..E?u....=;.....3..1....._..>.....v;.....r.|...y..C).....4..... .....@.....m. .....!.....@.....m. .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fortniteimg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	23766
Entropy (8bit):	7.581356595142999
Encrypted:	false
SSDEEP:	384:cfffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffW:cfffffffffffffffffffffffffW
MD5:	C6847419DC7E3E760E861EBFD07D3A8A
SHA1:	4A93394FC06F0C558E76013968C647D90AAE3CBB
SHA-256:	39F27EC2A484CC0E27D61CB1F5B930751A296F076B13E87C6788C47F5C57008F
SHA-512:	5EEB959CD86DCADF401CBCEDB2367EDF5D6137C9E933C63BE3BB4F0A2977A71554F6C872EAACA89D428414B243649B928F9333195B522FE0322341D0FAA061 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/fortniteimg.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fortniteimg[1].png	
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx...wp..}.....z#..V...(R..%J.$.X].c.r...+..q<q<..N2...x.O....k,.IY..-....b'...U$......?4{>...r..s..k.C.........>-.8.#....0 .u ....c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .. ...!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0........ ......c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!... ..0.............c. .....!.....0.............

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\fortnitetxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	25934
Entropy (8bit):	7.592505944467746
Encrypted:	false
SSDEEP:	384:zWv6T9SUokikcjPqsmRPh90EXBzm3ZjGR5SFsbYcP6c4OgH1NGsX5UEQX3Y2k:zW+9yk7cjPqJVHFmVG+OkdcwNGc5EXq
MD5:	F06708EF972EC74E089AE0030BFBB0E0
SHA1:	CDD5D038A6688513B0F8A480320449B13E402574
SHA-256:	B5784AB0F118A148A063A3AFA575B89E0A4025DD0F371719FFE4781B884CC852
SHA-512:	3CE747F09A38FA0882B74EC345A313E00967262483AC91375984CBBCD2BF5F0CFA87BFF8EEAD716CA1BFA519142C02E77DBB13E2E004A87405577E18DB873F7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/fortnitetxt.png
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx...wx.......@.H.. %....^..A)."(...QA.(5("..T8R.....r@... ......z/!.&!.)......fv....I.......w...y...cQJ).......rz............ ...@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC....... ......6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@. ...hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC............ .6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC.............6........@....hC....

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\httpErrorPagesScripts[1]</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>UTF-8 Unicode (with BOM) text, with CRLF line terminators</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>12105</td></tr>
<tr><td>Entropy (8bit):</td><td>5.451485481468043</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f</td></tr>
<tr><td>MD5:</td><td>9234071287E637F85D721463C488704C</td></tr>
<tr><td>SHA1:</td><td>CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152</td></tr>
<tr><td>SHA-256:</td><td>65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649</td></tr>
<tr><td>SHA-512:</td><td>87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>res://ieframe.dll/httpErrorPagesScripts.js</td></tr>
<tr><td>Preview:</td><td>...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\icon_facebook-93dcea8762[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	410
Entropy (8bit):	4.579347256654644
Encrypted:	false
SSDEEP:	12:t4NlfGqxGm1RVL7/PSeSfMENGGefikm+zZ2eW+BRe:t4NlfhrD3lEGDikmO5W0e
MD5:	BA789F0FA76D2FE62C6999EA65949734
SHA1:	3C90AE9C9D4904E5E47EDB1F845792CAB011AB66
SHA-256:	009EAC3D155EE41BD29906CCE01574C7B8C33967DA8ADF5E93557F50EEDD9899
SHA-512:	85633C3E4AE646C1085DC5039EE25466071B95BDF2F4617D4DECDF37D4CDBCB9588FFE66859B9968C9467EC5A3FB8ED8DAED0FEC4B5BEC189A2B55AFF68BD 516
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://statcounter.com/images/icon_facebook-93dcea8762.svg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\icon_facebook-93dcea8762[1].svg	
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="28" height="28"><path d="M26.348-.384H1.645C.798-.384.112.302.112 1.15V25.85c0 .846.686 1.533 1.533 1.5 33h13.3V16.63h-3.62v-4.19h3.62V9.35c0-3.586 2.19-5.54 5.4-5.54 1.532 0 2.85.114 3.234.165v3.748l-2.22.001c-1.74 0-2.077.827-2.077 2.04v2.676h4.15l-.54 4.19h-3.6 v10.753h7.076c.846 0 1.532-.686 1.532-1.533V1.15c0-.846-.686-1.533-1.532-1.533z" fill="#fff"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\icon_language-f261c0d39e[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1576
Entropy (8bit):	4.1470950598816145
Encrypted:	false
SSDEEP:	24:t4DWEgpX5dW4DLv6Ffe7wPiWPc++jAWfR6hAS3LNMfp1yL8lUz8i:2gpX55RBWPc+yf9S3LOfp1c8i
MD5:	24C58F338EFB1FFF60DBFCB2328EADD1
SHA1:	9A9BA7C79364E7BC61503023C94A1565E1E3259A
SHA-256:	0F2955D40959277EFDB0AE0ABE958C374AC693253AF04A312EB493733369C5B7
SHA-512:	C1C143716FED8F5FC4C22BE89C39FBA56734231BE14B78BEAAA59BE7EFB8AD88A884F2193F2F45430B145439DA386BD10AEB89F465FDE421D30143A956C919F 3
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://statcounter.com/images/icon_language-f261c0d39e.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="33" height="34" fill="#fff"><path d="M16.554.957a1.07 1.07 0 0 1 .141.011l.238.033a1.06 1.06 0 0 1 .243.064c.326.133 8.02 3.372 8.02 15.98 0 7.302-2.58 11.466-4.814 13.704 5.937-1.674 10.304-7.137 10.304-13.6a1.03 1.03 0 0 1 1.028-1.028 1.03 1.03 0 0 1 1.028 1.028c0 8.926-7.263 16.2-16.2 16.2s-16.2-7.263-16.2-16.2S7.626.957 16.554.957zm-12.487 22.8c.067-.033.143-.054.224-.054h4.452c-.464-1.653-.774-3.58-.837-5.814H2.44c.1 2.1.687 4.1 1.627 5.87zm11.487 6.716v-5.74h-4.3c1.248 3.184 3.1 4.908 4.3 5.74zm0-6.77V17.9h-5.6c.07 2.294.42 4.214.93 5.814h4.663zm6.853-12.612h-4.795v5.77h5.527c-.015-2.25-.294-4.158-.73-5.77zm-11.412-1.027h4.56V3.622c-1.275.9-3.323 2.8-4.56 6.442zm-.312 1.027c-.437 1.6-.718 3.518-.73 5.77h5.602v-5.77h-4.872zm12.444 6.797h-5.515v5.814H22.2c.507-1.6.858-3.52.927-5.814zM7.895 16.86c.013-2.2.26-4.112.663-5.77H3.953c-.053 0-.106-.01-.156-.026-.843 1.762-1.328 3.725-1.37 5.79 5h5.468zm-3.563-6.796h4.503c.9-2.978 2.285-5.042 3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\icon_twitter-b22ab5bb2d[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	723
Entropy (8bit):	4.201191230383513
Encrypted:	false
SSDEEP:	12:t46GqgeI7AugjE9WzUzSQ6Y4choJU/iehlYMTIv4Mez1PD+6hsAbRsqveP98Re:t46PEQUOQ61cua/dhlYMTIv4hF+6nbRk
MD5:	9A855D6AD9CD46CB2D45D26F6B32ACE3
SHA1:	EB334178FEFDF3321DD3482AD2EFD1F88B16EC26
SHA-256:	719E6F6C6C4F94B6FA414D799795312D56F15E360AF968E8677D8AC30608570B
SHA-512:	88C24D03668F00A7119275F1B593F0D2D8A53F2D42E7BDE17D44F4C6A8E823C99BFD103A527BABEBB7F9EFC87873122F1317A691DFC4D094710A411DDE32282
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://statcounter.com/images/icon_twitter-b22ab5bb2d.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="30" height="28"><path d="M9.118 26.13c11.195 0 17.317-9.374 17.317-17.502 0-.266-.005-.532-.017-.795a12.46 12.46 0 0 0 3.036-3.185 12.04 12.04 0 0 1-3.495.969 6.16 6.16 0 0 0 2.676-3.403c-1.176.704-2.478 1.217-3.864 1.493a6.05 6.05 0 0 0-4.442-1.943c-3.36 0-6.087 2.755-6.087 6.15 0 .483.054.952.158 1.403C9.34 9.058 4.855 6.6 1.854 2.888a6.18 6.18 0 0 0-.824 3.092c0 2.134 1.074 4.018 2.708 5.12a6 6 0 0 1-2.756-.769c-.001.025-.001.05-.001.078 0 2.98 2.098 5.467 4.883 6.03a6.04 6.04 0 0 1-1.604.216 6.01 6.01 0 0 1-1.144-.111c.775 2.444 3.02 4.222 5.686 4.272a12.13 12.13 0 0 1-7.559 2.634 12.28 12.28 0 0 1-1.452-.085C2.482 25.1 5.68 26.13 9.118 26.13z" fill="#fff"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jasondave[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 260 x 226, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	9696
Entropy (8bit):	7.891828280924392
Encrypted:	false
SSDEEP:	192:gAIdhHYIcKIOm8KKKKKKxKa3t0mQ156j66Xire8Mh555555e:OYYIOZTemo556ya5h555555e
MD5:	D9EC26E899118F3E3A122ADB42FBA32C
SHA1:	61D9D10C6AB96CE075DDD3E90D388B97BA2F0DEE
SHA-256:	6C6866681F549CF7F5F9985B8B2452BC133AB33045F3DE278A007A6E65822C58
SHA-512:	9B9ED470D0CD2335216EFE33C006ECDE52976633172EC889B111DA9CC9997FA41EFC77420378E08CE3683D853C8BABF20CED6B22B87EA45C1C863707954AE1 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/jasondave.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jasondave[1].png	
Preview:	.PNG.....IHDR.....b.!....iCCPICC Profile..H..W.T.....Z .RBo..*.....FH..%...bG..\.X..."....VD...X.?.QYY..XPy....v.=g..r..;..3...=K(.A.....bC...).LR7 .-..4.x.[,...PF.....H.... X.:._E.....@b N.....f.E.....df.P..!..A...q).cm)N..q2...@... SY,Q&.*R..Bv&..".h/....o...cq ~....<.U..[...'.o1.Gc.X..X..L.A|.0.5..\..-.9..9.a..Da.....b*...Q..k@|...K.}.$,Aa.....5...P.a.E@ ..1C.....,....Q...x.N...*....HE.e<n.....d.C.!....(..'.y.....(.U n.g.E(|.....FlD.X)gS..e.Bb.6.v.x$/....k..+...}.d.89r.....,.q....7.VW@..D.....ssBc.....$.51F1.. &^..GA$..A..$...<...-}.}.|$. ...d...UhF<.d#....E.O..@<.. ..B..2...mA.l.P...A....>.....~.9....SudVb01..F.!Z..`C.9....."`..I..Fr.....FxB.M.$.....,.j..X..s&..:a..Ev..g..C..x....C.8.....3.....@...%.....IY...B.b..`.>.... Z..%.5..>.GKl.v.k..`W..X-`b.:..;#...TV.#...e.8....j.^..?..R./]/q.wV.t3...g.....?<...p..n.....?:.2dg6..M.....R....c..p.....o:.7..W.p..-...u.....].....8.W...@0...A<H....@..<...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery-2.1.3.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	84320
Entropy (8bit):	5.370493917084567
Encrypted:	false
SSDEEP:	1536:AP1vk7i6GUHdXXeyQazBu+4HhiO2wd0uJO1z6/A4fGAub0i4ULgGiyz4npa98Hrb:z4UdWJiz6UAlJ8pa98Hrb
MD5:	32015DD42E9582A80A84736F5D9A44D7
SHA1:	41B4BFBAA96BE6D1440DB6E78004ADE1C134E276
SHA-256:	8AF93BD675E1CFD9ECC850E862819FDAC6E3AD1F5D761F970E409C7D9C63BDC3
SHA-512:	EDA31B5C7D371D4B3ACCED51FA92F27A417515317CF437AAE09A47C3ACC8A36BDBB5A5E70F0FBFD82D3725EDF45850DDE8CA52C20F9A2D6E038B8EAACEEB 3CF1
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-2.1.3.min.js
Preview:	/*! jQuery v2.1.3 | (c) 2005, 2014 jQuery Foundation, Inc. | 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:t his,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l=a.document,m="2.1.3",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:"",leng th:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a); return b.prevObject=this,b.context=this.context,b},each:function(a,b){return n.each(this,a,b)},map:function(a){return this.pushStack(n.map(this,functi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\logo_48[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	2228
Entropy (8bit):	7.82817506159911
Encrypted:	false
SSDEEP:	48:4/6MuQu6DYYEcBDlBVzqawiHI1Oupgl8m7NCnagQJFknwD:4SabhtXqMHyCl8m7N0ag6D
MD5:	EF9941290C50CD3866E2BA6B793F010D
SHA1:	4736508C795667DCEA21F8D864233031223B7832
SHA-256:	1B9EFB22C938500971AAC2B2130A475FA23684DD69E43103894968DF83145B8A
SHA-512:	A0C69C70117C5713CAF8B12F3B6E8BBB9CDAF72768E5DB9DB5831A3C37541B87613C6B020DD2F9B8760064A8C7337F175E7234BFE776EEE5E3588DC5662419D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/api2/logo_48.png
Preview:	.PNG.....IHDR...0...0.....W.....gAMA.....a.... cHRM..z&.....u0...`..:....p..Q<....bKGD.....C.....pHYs.....IDATh...P....=..8.....Nx. ..PlP8..;.C.1iL#6...*.Z..!.....3.po .o.L.i.I..1fl..4..ujL&6$.....w.....,Z..z. ~.....\.._.C.eK...g..%..P..L7...96..q....L.....k6...*..,xz.._.....B."#...L(n..f..Yb...*.8.;....K)N...H).%.F"Ic.LB.....jG.uD..B....Tm....T. .).A.}D.f..3.V.....O.....t_..].x.{o.....*....x?!W...j..@..G=Ed.XF.....J..E?../]..?p..W..H..d5% WA+.....)2r..+..'qk8.../HS.[...u..z.P.*....-.A.}.....I .P.....S....\|...)..KS4....I.....W...@....S. s..s..$`.X9.....E.x.=.u.*iJ.....k.....'...!.a....*+.....(...S..\h....@.....I.$..%.2....l.....a.|.....U....y.....t..8....TF.o.p.+.@<.g.....-.M.....:.@..(.....@.....>..=.ofm.WM{...e..,..D.r.. .....w....T.L.os..T@Rv..;.....9....56<.x.....2.k.1....dd.V.....m..y5../4|...G.p.V.....6...}.....B.....5...&..v..yTd.6...../m.K...(.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\matt-punchbowl[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 400 x 400, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	33340
Entropy (8bit):	7.958118061427431
Encrypted:	false
SSDEEP:	768:XsM7XJnUCqXNoP9I9tKkgA0tPvwW23u1gKken7Ynp0xtW3M:cM7XmVk9QckgAC4W2C/n7Ynp0xtW3M
MD5:	43258CBFFE9BB48B1E88A0F010644425
SHA1:	8B0D14E9E1766C42A49DCFA1E6F9A77430541C30
SHA-256:	28017199CB0C4ACC37B785A0050B77F39DCA5253DD6D7C260F4DF4227C26E5DB
SHA-512:	1D0542A9EDD13FCB9D238956FC5A3101CDCBC36E5E49DA20A5C071C0D1C474436AF2D0C10812AD6A2C19B54E1684337C7223107E14CCAA8ABF5CD4829952A C7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/matt-punchbowl.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\matt-punchbowl[1].png	
Preview:	.PNG.....IHDR.....6... .IDATx.....e}.....93'{...@.#....T""C.....u.8Zk.Z[.....kU.*E.`..B.. ...H. ..s.....hK[.$'9#..#.$I.d7.$I.$.."I.$Iv.H.$I.. .$I.d7.$I.$.."I.$Iv.H.$I.. .$I.d7.$I.$.."I.$Iv.H.$I.. .$I.d7.$I.$.."I.$Iv.H.$I.. .$I.d7.$I.$.."I.$Iv.H.$I.. .$I.d7.$I.$.."I.$Iv.H.$I.. .$I.d7.$...E<E<...?.....`...F..i"I.....d...F.7F..$..H.....,.....9"...x.?....o.....p/.....%p....@@. ...0."...X..@.....2 .....X.aMG..J....'F~..I.0..+.$..D.. ..0.....(y..-.8..x.)..N.8j..gM;hsO.....8`...GT2..@.c...8).1.u.....E.....=....<r...m^...vP[4cE[..K.D...E4#I...$..]..@..<..#..PW. ...g.A_>..I..fD.iHS.....0...J3..e.o.S..N.....`@&!....4xG...b..I..1>..E.6.1>$.2.....38....`.H.~#.d.p...1.d....s..z.cK....<.....6.i<...U.x&..^..Q#.".&..H.~.s`f<.x.Q#.`....4.&6T...D...U.. *.V:XQ...CKV?..'...E.d..I..x..+..P.:.0.\.~.....sZ.....-..E4$..Q.%Tc.....0@....0....v)..`.`B}...."..-..C.E^.....o.....7F.!.hX.F..."I.....K.5.....L..0.{..Z.....l. 7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\newform[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	12525
Entropy (8bit):	4.935801116629552
Encrypted:	false
SSDEEP:	192:K0CuirzMIF9MDq4jFgSXIznmOovTnCEDzaRwSY9fvGvDV9+g:CxrR6dXXwnKCWz2r
MD5:	CA27035C9D4F8CC35DE277C61667CAC1
SHA1:	52069F033797F07F33CF6E72D0BFD54AFF446E62
SHA-256:	EC237B3AF8BF0E9A44CC4223D05BB2DEA5BA5507BF29CFC0CC5F45FACE6B1882
SHA-512:	710C0DF3C6BA3D2B66DC80901C1B1B74AFEB6305FDEE2CAD7A6458DAE3E9F53DEA132F1F394045F00CB81FB47A06E50EE8A0839E1D07E7BF4FE40581C93ECD3D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/css/newform.css
Preview:	.w-layout-grid_fb {. display: -ms-grid;. display: grid;. grid-auto-columns: 1fr;. -ms-grid-columns: 1fr 1fr;. grid-template-columns: 1fr 1fr;. -ms-grid-rows: auto auto;. grid-template-rows: auto auto;. grid-row-gap: 16px;. grid-column-gap: 16px;.}...success-message {. border-radius: 3px;. background-color: #22d469;. color: #fff;.}...button_fb {. margin-top: 20px;. padding: 15px 40px;. border-radius: 40px;. background-color: #dd2476;. -webkit-transition: background-color 200ms ease, background-position 200ms ease, color 200ms ease, border 200ms ease, box-shadow 200ms ease;. transition: background-color 200ms ease, background-position 200ms ease, color 200ms ease, border 200ms ease, box-shadow 200ms ease;. font-size: 13px;. font-weight: 600;. letter-spacing: 1px;. text-transform: uppercase;.}...button_fb:hover {. back ground-color: #ff512f;. box-shadow: 7px 7px 23px 0 rgba(0, 0, 0, 0.2);. color: #fff;.}...button_fb.gradient-submit-button {. height: 50px;. margin

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\noahkagan[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 688 x 688, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	127554
Entropy (8bit):	7.961380529289356
Encrypted:	false
SSDEEP:	3072:R55cLurjbYyxonnUaLV/xFOBXIjecEKtMMdO1f4Nb2Vpw:R4LAYhnVLVKuECbdog2zw
MD5:	ECB8D4A0C253344FC9031C1FE54BA0AB
SHA1:	37EE1CFF43077C52D5CBBF7241E1B8A504A94944
SHA-256:	5C0611C894E4FFE2928B7E634C3C4709F9B19E5CCDB04A18B6DC92775EF69CE7
SHA-512:	BC3BCD8EC8C00403A05BF007033518CE3B42928D5F77E820B4F32870B0B190397C6BD47B3E6F69C259BE3E5990B3BBE1DEAF9827C09D69DB62D9772503B2E4DB
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/noahkagan.png
Preview:	.PNG.....IHDR.....`DL.....iCCPICC Profile..H..W.T.....Z .RBo..*.....FH..%...bG..\.X..."....VD...X.?.QYY..XPy....v.=g..r..;..3...=K(.A.....bC...).LR7 .-..4.x.[,...PF.....H.... X.:._E.....@b N.....f.E.....df.P..!..A...q).cm)N..q2...@... SY,Q&.*R..Bv&..".h/....o...cq ~....<.U..[...'.o1.Gc.X..X..L.A|.0.5..\..-.9..9.a..Da.....b*...Q..k@|...K.}.$,Aa.....5...P.a.E@ ..1C.....,....Q...x.N...*....HE.e<n.....d.C.!....(..'.y.....(.U n.g.E(|.....FlD.X)gS..e.Bb.6.v.x$/....k..+...}.d.89r.....,.q....7.VW@..D.....ssBc.....$.51F1.. &^..GA$..A..$...<...-}.}.|$. ...d...UhF<.d#....E.O..@<.. ..B..2...mA.l.P...A....>.....~.9....SudVb01..F.!Z..`C.9....."`..I..Fr.....FxB.M.$.....,..j..X..s&..:a..Ev..g..C..x....C.8.....3.....@...%.....IY...B.b..`.>.... Z..%.5..>.GKl.v.k..`W..X-`b.:..;#...TV.#...e.8....j.^..?..R./]/q.wV.t3...g.....?<...p..n.....?:.2dg6..M.....R....c..p.....o:.7..W.p..-...u.....].....8.W...@0...A<H....@..<...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\opt-out_button[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 87a, 186 x 27
Category:	downloaded
Size (bytes):	2832
Entropy (8bit):	7.8224749711595045
Encrypted:	false
SSDEEP:	48:Ri5rZtspAUyj3TxaluWl3c0K4n63J6TffxWvkvq81LK/+x8dJRnfN5xdixc:85rZtrUyFaluWRc0Ke63UFWMv3W/+x87
MD5:	FC1E4CEDDF3676B64062A3D7ABC6FAC8
SHA1:	E45DC76AD8A97F1DDF6DF03BDDBEAF86CF71347D
SHA-256:	576D05B6E3CA0FC2FE5C4212AF378408C14CC061D028CD1FB277F75A0B87C389
SHA-512:	A3B3A56DFE1846C1264FEB89B63F5399DDA13BE9B365F4A62B6BD92C59EFFFC9CC1ECCAD5DF2DAEC2BB82F6F6690D159D535A06F7AA56A3AFA530A358E0BFA44
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://statcounter.com/images/opt-out_button.gif

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\opt-out_button[1].gif	
Preview:	GIF87a.....%%.--.....,.,.,.-....w...++.....++.,-.....++.....h....AA.....#"...BC....,-.ss.pp.TS.,+.GG.)).TT.ED...,-...[[.~~..o.{{....,+....,+.66.99.bb.fe.;;.....-...x"..t.wv.....)).,-....XW...XX.%%.&'.54.dd.--....TU.....AA.66.....oe.,+.++...MM.kk.++.,,.OO.FE....99.,,.((.((.''.++h...0/.,,....QQ..o.cd.h^...M...W..d.OP.^^.....((....f...,.....<.S.....5.5.S"<.....3.X:..ZTS5....._TZ....qt..IS.@@....._YI...sHD. _$8...g..P9X.I:..1"..Dc.t.,r.I."G..?..V2c./Kn.92&.*<d..jP.#r . .....DQ....PU..:5.S$M.,.Z u.S.V.Vu:.l.W..=....n....'l..>?.pR.Q..x.....Z..b.Z.Kn...b.o.k..y.a.3g.,.rg.G.N.8.....J...~...B&.....N.....+_.9p.f$...`F...,jT.....u....>>.y.....O.:q6..N.6..G.....h`.Y.0.....F(..VX... ."..nL...78h!.....fh0..~.a.~....C.....'....<..#.<.....q".. ...K..d.:Bi..TB...\....?....Kd ".=....M.`e.>..c. ...p.(...D`../.7....1..h&.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\otnuxQi5Wy3Eq9ZSf6m85_p8wZJ2BK7uby0VQVvK-UA[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	21037
Entropy (8bit):	5.578581267912917
Encrypted:	false
SSDEEP:	384:K3MOZGdqZx3F1oAes+SyMvrTc03QMEZguFhhqYj8OEM5lWmR65hLzjzDzEzOYP:KcjsZx3F1oAB+SVrTc03nErxxzlUb0h
MD5:	7AD08192F8856DD00BB2A2F2186E231B
SHA1:	257BCF4051EAA0DF2BEA75DA9BDC89A2504E9BA6
SHA-256:	A2D9EEC508B95B2DC4ABD6527FA9BCE7FA7CC1927604AEEE6F2D15415BCAF940
SHA-512:	50358F70890EF9BF5EEC3D6D3856809FA5513A91C2810F188BD613131513ADA93576AEBBC3FDB9D860C2F53710639E526E8CB20123FA726C047B6665E8505A6B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/js/bg/otnuxQi5Wy3Eq9ZSf6m85_p8wZJ2BK7uby0VQVvK-UA.js
Preview:	/* Anti-spam. Want to say hello? Contact (base64) Ym90Z3VhcmQtY29udGFjdEBnb29nbGUuY29t */ (function(){var n=function(y,g){if(y=(g=null,v).trustedTypes,!y||!y.createPolicy)return g;try{g=y.createPolicy("bg",{createHTML:T,createScript:T,createScriptURL:T})}catch(k){v.console&&v.console.error(k.message)}return g},T=function(y){return y},v=this||self;(0,eval)(function(y,g){return(g=n())&&1===y.eval(g.createScript("1"))?function(k){return g.createScript(k)}:function(k){return""+k}}(v)(Array(7824*Math.random()|0).join("\n")+'(function(){var W,yL=function(y){return y},gY=function(y,g){function v(){}((y.W=(v.prototype=g.prototype,g.prototype),y).prototype).constructor=y,y.DU=function(T,n,k){for(var P=Array(arguments.length-2),M=2;M<arguments.length;M++)P[M-2]=arguments[M];return g.prototype[n].apply(T,P)}},u=function(y,g){return"object"==(g=typeof y,g)&&null!=y||"function"==g},vq=function(y,g){if(y=(g=null,J).trustedTypes,!y||!y.createPolicy)return g;try{g=y.createPolicy("bg"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\packetimg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	127613
Entropy (8bit):	7.961308629068017
Encrypted:	false
SSDEEP:	3072:6atTYCdAaSFqZRf8KBWrqbC8+wojkyepYiE4vIa6FeM0b:ttTFZR0clbv+/jcpRlNMe
MD5:	9F7BA7F03E56D2E10B3CE1805B5284BB
SHA1:	ED25151943F74E21D70EE55A5C1CCA5FAAFB9AC0
SHA-256:	C04E10243778820101E08708075C5C00376BACD0C3587CCF2593D703D97718DE
SHA-512:	70F1B73899A4829CAA8B3B756A513BEFC16C8CD2BCA567A2F0FB5BE11113C8D8DDC6BC997FE8FFEDE127AD68716BBE83CBE16F64ABBF37A87FE203974009E18A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/packetimg.png
Preview:	.PNG.....IHDR... ... .p.h....sRGB.....pHYs.....+.... .IDATx....\G~...yNU.....d.M.....l+z..cb..y1/.~..y.....v.....+@l.~..]..d..<U.....A..Bm.N.|2..e).$...../.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\packettxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	23674
Entropy (8bit):	7.549601659992931
Encrypted:	false
SSDEEP:	384:eShQTiH899IQD3BHmjskysaJ5M9TMALHchHUOlHuANQwidAwhgTk:DhQ+cvzBHmjlaJ5M9TMRRQANQ1dAwhgA
MD5:	65B140A330AFD263E3A2A6B07FCB3158
SHA1:	4CE06EC00D655B4866D1516C7716292E69145D52
SHA-256:	055C532BBE959A11310303F3CCBF1952284C447FC0F4484427DACC728104304C
SHA-512:	7DCBD179720337299D00DB0B6C4E62CA15D6EAA2552F3CF0AD8FF981C43685E01136B62297971039CD41191B3C17D5D4E73A71C87636F0303030137A7672CFF0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/packettxt.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\packettxt[1].png	
Preview:	.PNG.....IHDR... ... .p.h....sRGB.....pHYs.....+.... .IDATx...y|M....O.ID.I.E.A.)jVS..T.....ZZ5..^C....U-.. ...j.5.....g...s/..gJ. ...q.Yg..}N..g..RJ.....h.....u.@....hC.....6.....@....hC.....6..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\paulgyc[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 257 x 257, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1080
Entropy (8bit):	6.91354721800723
Encrypted:	false
SSDEEP:	24:Pq13s3HGVjrC8xTToFhDjTX2XNHNkpLw2oG:PqVwGVPHiDjD2XNSpU2oG
MD5:	F763CED5785D6FB77E39631F74DBCFBA
SHA1:	FB889E2E459A160D540BDC2D35CEA2DBCE48B7D4
SHA-256:	7481412385FE6D0F7D4A3339D90FE12309432CA41983E8D350B232301D5D8684
SHA-512:	3E382D2016C267CE605B2BD1131121A9F4EF065718B1309596A05942216EF5668E812DCC9D2C7DC5FDA2E5FD11D5D2ABF8207249CB3C85F0E37597892930846F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/paulgyc.png
Preview:	.PNG.....IHDR.....O2.....BPLTE.e".e".e".e".....P.....i.x7.....o,..\.C.....u.....e".2._....tRNS.@.` '.31....IDATx^.....0.. |.....a ...P.....}:...g.n.. ..j.@..c..|.Q....@....@....@....@....@....@....@....@....@....@....@....@....@....@..G....z1..*p..q..f.y.*0._.Vo..`.x.."..%P'.h".y....E..xL-p....6..XD...\.\..5.*..U@G.O`...<T...J.].....@....;...!p....F.....T...&.....1...H.?..@@...O .....@(...."&...z -..z0.*'p$.@@F.J .....+.o..GP.*.$.E.....@..5....hAo...".bX..pD ..*0>E.....@.....&..#..@h.z5.....(..R..@.$....U.@...H .@..A3.....v.E..G..*.'.Wru$.P..E.:...$....@&...:..@.-.Wru$.E...#hV).@...V..]@G.9..%...t....U.N....G.Z..:..@:..".$.....I.E@Gp.L..\|u.\|..O.@J.c...biR...b.U;.....'.R..t..2.....d.:...V%....h3.8.@.....\|.:.;.....@...).....q..QD..-..]$.^@G....t.md.....c.....,#..^...[.T.@f....f..N..... ....m.....@....@....@....@....@....@.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\scroll-with-stickynav-inline.jquery[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	658
Entropy (8bit):	5.065415362707859
Encrypted:	false
SSDEEP:	12:891RZvsR/9Xhk3Kne26Nt2W1chO68Oy5C66PvaMTKEx+xKFMcszOa6RmytsivKPM:GvsRz4KniHC981C6OaMuEIxUM3zO1wKx
MD5:	333D9FEB63060E511E03B9F122914F27
SHA1:	F6D278B9D42DF1BD8B53F646CD8E89FCEBC88102
SHA-256:	D93563EE114D7C35896F38A11CC02696B91B4FA21641DABC0523EDF7913020CB
SHA-512:	CEF7A709C640098A8D414957EE609D9235467F8645843FC630547106359760382E60937477A2A05BAFFCD9EF2FD405CD170E4B9CCD62DF4E3EC1E592F1668944
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://statcounter.com/js/scroll-with-stickynav-inline.jquery.js
Preview:	jQuery.noConflict();.jQuery(window).load(function() {...function scrollToHash() {...var hash = location.hash.replace('#',''); // not all browsers include the hash, so remove to have a good baseline...if (hash != '') {....if (jQuery('#' + hash).length > 0 && jQuery('.sticky-nav a#' + hash).hasClass('link-anchor') === false) {.....var hashOffset = jQuery('#' + hash).offset().top;.....hashOffset = hashOffset - 82; // 82px is height of sticky-nav.....jQuery('html, body').animate({scrollTop: hashOffset}, 1000);....}...}..}...jQuery(window).on('hashchange', function() {...scrollToHash();..});...scrollToHash(); // called when the page is first loaded.});.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\speechkit-iframe-helper[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1701
Entropy (8bit):	5.174284375262848
Encrypted:	false
SSDEEP:	24:25dqs4B/gzbihdd1vwhMieTw0Edvyz6RWjiuH+UiPGl272omCzfI7k0Q7fPFQTY3:cdqsHzhMbkjwoeIHZKk77nIoht
MD5:	9EE77BC97A26521CA9D97BB04EA0DD0D
SHA1:	45B2BDD8C5D96F88AD8F04C6C5BEB51D8A4E232A
SHA-256:	3AA8022D438C33B360E2E6332748D4B784A6A660311A236412BCE652D9DF9251
SHA-512:	27FBEECF5873FF65D2D70A46AC32EF8BBD2C588A0535DC3447C4020442E098CE71463A89293685080251D767159FC529A522B9F2A838A823024D3C45F35E3459
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.jsdelivr.net/npm/@speechkit/speechkit-audio-player@latest/dist/speechkit-iframe-helper.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\speechkit-iframe-helper[1].js	
Preview:	var speechkit=speechkit||{};speechkit["iframe-helper"]=function(e){function r(t){if(n[t])return n[t].exports;var o=n[t]={i:t,l:!1,exports:{}};return e[t].call(o.exports,o,o.exports ,r),o.l=!0,o.exports}var t=window.webpackJsonpspeechkit__name_;window.webpackJsonpspeechkit__name_=function(r,n,i){for(var c,s,a=0,u=[];a<r.length;a++)s=r[a],o[s]&&u.push(o[s][0]),o[s]=0;for(c in n)Object.prototype.hasOwnProperty.call(n,c)&&(e[c]=n[c]);for(t&&t(r,n,i);u.length;)u.shift()()};var n={},o={49:0};return r.e=function(e) {function t(){s.onerror=s.onload=null,clearTimeout(a);var r=o[e];0!==r&&(r&&r[1](new Error("Loading chunk "+e+" failed.")),o[e]=void 0)}var n=o[e];if(0===n)return new P romise(function(e){e()});if(n)return n[2];var i=new Promise(function(r,t){n=o[e]=[r,t]});n[2]=i;var c=document.getElementsByTagName("head")[0],s=document.create Element("script");s.type="text/javascript",s.charset="utf-8",s.async=!0,s.timeout=12e4,r.nc&&s.setAttribute("nonce",r.nc),s.src=r.p+""+({}[e]||e)+".js";var a=se

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\statcounter-b87c6b0ce8[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	65621
Entropy (8bit):	5.223443383885181
Encrypted:	false
SSDEEP:	1536:Xfd3ioFpY59PDQEny+8VgYYlmv/AyFsU4ipDAGtl9:Xu5RdU4czt3
MD5:	59ABE8015A274B6AFFFC4795A5CA5A3C
SHA1:	55825BD4490F67615F37622ABDEFEADEE8F60B12
SHA-256:	0492E5D36BCE853E39C3D2DC1B12B8202DB903365487AA94DE309499E3CEAD29
SHA-512:	24F07377C32ED8065CC07B1358326F87F3571D9CD92D32470EEA852D98C7510D963290843FDD4FF558D09DFA9E6D18ECEF4442EBB9F1688618791419519D043A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://statcounter.com/js/packed/statcounter-b87c6b0ce8.js
Preview:	/***.. (c) 1999-2021 StatCounter. All rights Reserved... THIS FILE IS AUTOMATICALLY GENERATED..***/./*! jQuery Validation Plugin - v1.15.1 - 7/22/2016. * h ttp://jqueryvalidation.org/. * Copyright (c) 2016 J.rn Zaefferer; Licensed MIT */.!function(a){"function"==typeof define&&define.amd?define(["jquery"],a):"object"==typeof module&&module.exports?module.exports=a(require("jquery")):a(jQuery)}(function(a){a.extend(a.fn,{validate:function(b){if(!this.length)return void(b&&b.debug&&w indow.console&&console.warn("Nothing selected, can't validate, returning nothing."));var c=a.data(this[0],"validator");return c?c:(this.attr("novalidate","novalidate"),c=new a.validator(b,this[0]),a.data(this[0],"validator",c),c.settings.onsubmit&&(this.on("click.validate",":submit",function(b){c.settings.submitHandler&&(c.submitButton=b.target),a(this).hasClass("cancel")&&(c.cancelSubmit=!0),void 0!==a(this).attr("formnovalidate")&&(c.cancelSubmit=!0)}),this.on("submit.validate",function(b){fu

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\styles__ltr[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	51178
Entropy (8bit):	5.968129596292632
Encrypted:	false
SSDEEP:	768:+LUmmAWTe2uXYp8Mi+yKSrKebyBwxDl+xedtY5PoiDH1fkQJVEwY:4UcW6v+2rKwxDliP7dnY
MD5:	E548DC0AEF0A21A2DF5B964EF93118AA
SHA1:	983091AEC1E7BFEB79F768E4B997C43B55EDE14A
SHA-256:	6B08EA3A348838BC942AD470A757575975BD09459B63C1872C6E1129A6CA1939
SHA-512:	17A4EC0CB167C2C7653ABEF6384C68BE2BCEEE6FB657D3A27132B3508F28087AEEB8072409DB95F6D4BE7BFE1F54A51D6EB073AE5D902DA90ADA5ECDE72F2 9FC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.gstatic.com/recaptcha/releases/jxFQ7RQ9s9HTGKeWcoa6UQdD/styles__ltr.css
Preview:	.goog-inline-block{position:relative;display:-moz-inline-box;display:inline-block}* html .goog-inline-block{display:inline}*:first-child+html .goog-inline-block{display:inline}.rec aptcha-checkbox{border:none;font-size:1px;height:28px;margin:4px;width:28px;overflow:visible;outline:0;vertical-align:text-bottom}.recaptcha-checkbox-border{-webkit- border-radius:2px;-moz-border-radius:2px;border-radius:2px;background-color:#fff;border:2px solid #c1c1c1;font-size:1px;height:24px;position:absolute;width:24px;z-in dex:1}.recaptcha-checkbox-borderAnimation{background-image:url(A/wD/AP+gvaeTAAAACXBIWXMAAABIAAAASABGyWs+AAAACXZwQWcAAABUAAADSAC4K4y8AAA4oElEQVR42u2dCZRV1ZX3q5iE4IQIiKQQCKBt0JLEIUZwCCk 7pBNFiRMajZrIl9aOLZ8sY4CWdkDbT2McooaEmNixFhpaYE2dCiLScWiQHCgoGQoGQuhGArKKl7V+c5/n33fO/V4w733nVuheXuv9V/rrnvP2Xud3zvTPee+ewsKxMTEx MTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExMTExP4OdtlT6ztAbRWvvLy8A3QkwxzH6tBGMMexI

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sumologo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	27706
Entropy (8bit):	7.519032809544115
Encrypted:	false
SSDEEP:	384:lwultvOaOcvdhTQc1NJ9XCiordsUnV9di0y6XFn/bNuJJuTxqyesk:lwufOghTQq9ydrdsUV9diyXFpldbeD
MD5:	C266D42F77BFDDCB3FC689D64CE1906A
SHA1:	4AF7E75CD940CB44728AAD28964A71036965B2A7
SHA-256:	26E65C354A621FED60FEEF1C2744A46291A5E9DF8D5B6E104BACB524F70B53B7
SHA-512:	E01BAB1F3A843B7D18320381600104F4E67B3A3158E117C813E7CAAAFA56E7E0C8844D06B395FCE1DB95D57824A1180FCDC1516D66D0258D7676D0DBD44AD4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sumologo[1].png	
IE Cache URL:	http://https://assets.superlander.com/images/sumologo.png
Preview:	.PNG.....IHDR... ... .p.h....sRGB.....pHYs.....+.... .IDATx...w.....}).T..X..1FM1&....c.-j..B..%.E.=vE...w.!EDE...}o....c.]...{X..z.<....e...=.1.....>....k.....k. ....!.. .....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....! .....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....! .....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. ....!.....k. .... !.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sumotxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	24342
Entropy (8bit):	7.556905589280666
Encrypted:	false
SSDEEP:	384:Pm6GQ5IBMLjCDyMZUi1ioAdsTg3UfgvqQbvCyXBEzMpcb56Vk:+fnBMaDzZXAdsTKUWblV06q
MD5:	1C5976EC5594C2F84005AEDE17FFF1CF
SHA1:	D01D9EB204C0464F8EF84B25A9BF7265A60A3E27
SHA-256:	A0C667A4EC3FBB528421EED383B5F0D8DD69F1DF62ED9CD17982F6586F0A41C8
SHA-512:	3BD136129D5BA4487FE9B5BB6536C1B4E32B754FFE30F81C21C32D57026781B15CA76047DD5FD0EA2E15D88A649F22A99E4DCFCD88863F164B7066CBF47FA5F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/sumotxt.png
Preview:	.PNG.....IHDR... ... .p.h....sRGB.....pHYs.....+.... .IDATx...y|M.....BRbH....V..<....R.mU....R...V.;...US.^CiQ...D..yVD.b.....G....O.$}=.....>k..d..,J)%.....m. .....!.....@.....m. ....!.....@.....m. ....!.....@.....m. ....!.....@.....m. ....!.....@.....m. ....!.....@.....m. ....!.....@.....m. ....!.. .....@.....m. ....!.....@.....m. ....!.....@.....m. ....!.....@.....m. ....!.....@.....m. ....!.....@.....m. ....!.....@.....m. ....!..... ...@.....m. ....!.....@.....m. ....!.....@.....m. ....!.....@.....m. ....!.....@.....m. ....!.....@.....m. ....!.....@.....m. ....!.....@.. .....m. ....!.....@.....m. ....!.....@.....m. ....!.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\t[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	162
Entropy (8bit):	4.996037359355885
Encrypted:	false
SSDEEP:	3:YTX/6ABZH9klgTH2ILLg6M5CA5EfMJJJv4+TzKUUaXWkYkWnt39jrj:YbvBQZ7McGTHV9zaalgD
MD5:	E78D89ECEE82B9B1CCC7DFDB61D776E1
SHA1:	B714CC4738BE371C4FFC25658A20EE285C6EF326
SHA-256:	0564D20C6662FA83C89B22EF3E1185CEDE3D6E4DFBC1525E936930E8EA58FB13
SHA-512:	44E28A6692DBEDDDC6B58A70712E04EAA54B1652F73630DB678AADB6FD4E8989C9D78DD6CC8A84F0795FDE2544F2CF5F0F9D320FE75460153A1CA385B3928C6
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://c.statcounter.com/t.php?u1=709773700B414F8260AA3A899DF3B834&sc_project=11965032&java=1&security=3c896546&sc_snum=1&sess=830817&p=0&rcat=d&rdom=d&rdomg=new&bb=1&jg=new&rr=1.1.1.1.1.1.1.1.1&resolution=1280&h=1024&camefrom=&u=https%3A//certc.com/&t=CERTC.COM%20is%20available%20for%20sale%20or%20other%20proposals&invisible=1&sc_rum_e_s=3025&sc_rum_e_e=3435&sc_rum_f_s=0&sc_rum_f_e=2104&get_config=true
Preview:	{"visitor_recording":0,"time_difference":"1800","counter_image":"data:image\/gif;base64,R0lGODlhAQABAJHVAP\/\/\/wAAAMDAwAAAACH5BAEAAAIALAAAAABAAEAAAICVAEAOw=="}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\twitterimg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	37154
Entropy (8bit):	7.9084538039084515
Encrypted:	false
SSDEEP:	768:hdEAYHRUt1oPt2EdgLSOMKUGnDPXgjGj0hBQS7bNo:sAYHeykSOfUGnUjGj04
MD5:	30FA8BF90C54DA65D9310C385803C2CF
SHA1:	04D803FCB7E83485A849A9FE6FC4138D75347226
SHA-256:	6B6B96DDF281F71A022F0B288AF3C65DDFE5A30F8D8C77A5C98C8E840DDA7967
SHA-512:	CD9093F2D8C404EA52FB330C9BAB6D585A85DCB0CA5F096D011308A30B4FC098E4087DFA8DAADD0B38CB3F4C649BD4BF4D8C6EE079C7478CE42BD9EDEF05F55
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/twitterimg.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\twitterimg[1].png	
Preview:	.PNG.....IHDR... ... .p.h....sRGB.....pHYs.....+.... .IDATx.....y.....}.V ..."..%..$[.....g....v[.v.-..)....P.5.....$..".K>.s..WE%2.o.{.7ED I.$I...{.$I.$....$I....@$I.$u.."I.$.3..I.$I.1.H.$I..D.$IRg. .$I.:c..$I.....$I....@$I.$u.."I.$.3..I.$I.1.H.$I..D.$IRg. .$I.:c..$I.....$I....@$I.$u.."I.$.3..I.$I.1.H.$I..D.$IRg. .$I.:c..$I.....$I....@$I.$u.."I.$.3..I.$I.1.H.$I..D.$IRg. .$I.:c..$I.....$I....@$I.$u.."I.$.3..I.$I.1.H.$I..D.$IRg. .$I.:c..$I.....$I....@$I.$u.."I.$.3..I.$I.1.H.$I..D.$IRg. .$I.:c..$I.....$I....@$I.$u.."I.$.3..I.$I.1.H.$I..D.$IRg. .$I.:c..$I.....$I....@$I.$u.."I.$.3..I.$I.1.H.$I..D.$IRg. .$I.:c..$I.....$I....@$I.$u.."I.$.3..I.$I.1.H.$I..D.$IRg. .$I.:c..$I.....$I....@$I.$u.."I.$.3..I.$I.1.H.$I..D.$IRg. .$I.:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\twittertxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	24270
Entropy (8bit):	7.543593928692902
Encrypted:	false
SSDEEP:	384:fJOU2rv4SnRbMMMi3vkhAU8wCyOXgtyoxvbcBBFTxibBuEYc1zF8kaX5UqYwP2mA:SRbMMtzU2yOX9OvbeBFNibN91zFBaaqK
MD5:	C1C7995C898C8E2F79DEBC3F14F54BC0
SHA1:	FAE50CF18405BEB7A67637AF865DD64D78E319C6
SHA-256:	3DDFACC42AA590F4B5D8D1C8CAFF9E859E3D5BDF93760A3CB79ECED669ED8634
SHA-512:	B768B91F07C22FBAC9FFF522E2864B8198197BE4D2FD23F7AD6E32D59431E8F2F6ECDB96880C51FD05067519300440E846177439BB18CEE0A30E18311230CD08
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/twittertxt.png
Preview:	.PNG.....IHDR... ... .p.h....sRGB.....pHYs.....+.... .IDATx...yXU.....D E!s.L.S.Rs.....~.V..73...~..kf..r..5..T..rJ.2.K..7...Gd8..G?}...aa.~=.y.Zg..^.....(.....^%=..... ..m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. . .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....! .....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!..... .....@.....m. .....!.....@.....m. .....!.....@.....m. .....!...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\webfont[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	17698
Entropy (8bit):	5.495729910786858
Encrypted:	false
SSDEEP:	384:r1+WTmL6g/zeuhkyU4qT9/2XJFaFBmNycSlixrt8qb5ef2fHHQ/DYdZM:rcWTm/3kyQTlBjcS7zHHvZM
MD5:	82C1CB347D2F923A399C391B336F3A13
SHA1:	4C8CB9E43CF5C01E8AFD669C4264E924AA9EE7E3
SHA-256:	D142A29DFC233602672353F1BFAF7D8E72331EC6902D8DD12CB56E5EAF794FC2
SHA-512:	135439D74E31E4F6D0413C702B1ACC8D4DA98433051249ABCFB730E84701F1B49B70F2AF171763FC253D6F32F81A76642ABB9D4584A82856D92D911B4F40C28F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://ajax.googleapis.com/ajax/libs/webfont/1.4.7/webfont.js
Preview:	/*. * Copyright 2013 Small Batch, Inc.. *. * Licensed under the Apache License, Version 2.0 (the "License"); you may not. * use this file except in compliance with the Li cense. You may obtain a copy of. * the License at. *. * http://www.apache.org/licenses/LICENSE-2.0. *. * Unless required by applicable law or agreed to in writing, softwa re. * distributed under the License is distributed on an "AS IS" BASIS, WITHOUT. * WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the. * License for the specific language governing permissions and limitations under. * the License.. */.;(function(window,document,undefined){.var j=void 0,k=!0,l=null,p=!1;func tion q(a){return function(){return this[a]}}var aa=this;function ba(a,b){var c=a.split("."),d=aa;!(c[0]in d)&&d.execScript&&d.execScript("var "+c[0]);for(var e;c.length&& (e=c.shift());)!c.length&&b!==j?d[e]=b:d=d[e]?d[e]:d[e]={}}aa.Ba=k;function ca(a,b,c){return a.call.apply(a.bind,arguments)}.function da(a,b,c){if(!a)throw Erro

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\webworker[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	102
Entropy (8bit):	4.866417162271585
Encrypted:	false
SSDEEP:	3:JSbMqSL1cdXWKQKEIElWc800XwECWaee:PLKdXNQKslW903jL
MD5:	C4DE09C4DA7F5AC82A7022B16D6CA1E1
SHA1:	7B219909A24256D5BC57F6F25DFDDDB0DEDFEE43
SHA-256:	AB1E16C1B3F793E0AEC723C7A7ADD9E179781105D1646CED630AF7007CA52720
SHA-512:	3A22CB6A31BFBA24143351F018436FF7978C444A36392447D566C9251A37DE76ECF1262FE4EE2BB97EDD788481626A2AFB72FEFFCEE853FE2840A31C3A68F525
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://www.google.com/recaptcha/api2/webworker.js?hl=en&v=jxFQ7RQ9s9HTGKeWcoa6UQdD

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\webworker[1].js	
Preview:	importScripts('https://www.gstatic.com/recaptcha/releases/jxFQ7RQ9s9HTGKeWcoa6UQdD/recaptcha__en.js');

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\10YYSL0G.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	95835
Entropy (8bit):	4.725769390036305
Encrypted:	false
SSDEEP:	1536:JGIiWZPUJzvkXbjp8tLb5rf5mxZZza+O+4Isuy:JNiWZPUJzvkXbjp8xbxgZza+O+47R
MD5:	CD625CDD3135F670DDEE2AB57738CAEE
SHA1:	5FACB275C999337168EA72116D01385E14B67859
SHA-256:	B77402C4798015B23D78946D59742E8A8357DBEADFC8E8179DBD27B4E827B5BC
SHA-512:	2BA8FE1DD7233DB5C2CAEA48F21F0B6617C852E3989A307A5DE7254AAABA29D456A63742C2C5F6CDE86638968B7CE5296239F71BE08ED4B4317340116547B0D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://certc.com/
Preview:	<!DOCTYPE html>. Last Published: Wed Apr 24 2019 21:58:29 GMT+0000 (UTC) -->.<html data-wf-page="5ca64202783a9b91a5c5d9e1" data-wf-site="5c6caaa7255b5b35837464b2">.<head>. <meta charset="utf-8">. <title>CERTC.COM is available for sale or other proposals</title>. <meta content="A unique opportunity to secure CERTC.COM for your brand" name="description">. <meta content="CERTC.COM may be available for sale or other proposals" property="og:title">. <meta content="A unique opportunity to secure CERTC.COM for your brand" property="og:description">. <meta content="summary" name="twitter:card">. <meta content="width=device-width, initial-scale=1" name="viewport">. <meta name="robots" content="noindex">. <link href="https://assets.superlander.com/css/generic-normalize.css" rel="stylesheet" type="text/css">. <link href="https://assets.superlander.com/css/generic-webflow.css" rel="stylesheet" type="text/css">. <link href="https://assets.superlander.com/css/generic-landers.webflow

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
Reputation:	low
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\OpenSans-Regular-webfont[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), Open Sans family
Category:	downloaded
Size (bytes):	19836
Entropy (8bit):	7.968988367523068
Encrypted:	false
SSDEEP:	384:mMda71VygUA7pcFf0MYV+iP0kuqLtfBPUAiGBnOk8PhpU:my+ggUA76fY+iLjjtiAOva
MD5:	C4D82460EF260EB1589E73528CBFB257
SHA1:	A64C0E7003DD8EC5E9D265956DBADD6E8B12C155
SHA-256:	25F7C6430E4B537DFA6BBE5554D4641C0FBDBF3F9351AAB6CD91D43D11738528
SHA-512:	2A717D36D80183DDC1A8B2DE80E1C9370DC5FE751304507F5EB9C43A3BEF7E8764914AF06FB70328123404526F707A5AA55D97FEF9FCF56D998EB7305B837461
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://statcounter.com/fonts/OpenSans-Regular-webfont.eot?

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\OpenSans-Regular-webfont[1].eot	
Preview:	

|M...L.....LP....[.@(..... .....O.p.e.n. .S.a.n.s.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .1...1.0...".O.p.e.n. .S.a.n.s. .R.e.g.u.l.a.r.....BSGP.....
..l..4u.A..(D....xZW.h[qJ.x"c.r,g,E.&..C.....@.rX...Y..?&.....+.u...LFM.l...SM.P.....+".betT.R..1..U0.:~b...R.....bk.F}.SC....X\7j.)Y.}.R.#".Z.....AB.....UC.T.vm..a....i...R....xE....
|W).".....B.....K...a...0....#1h..G.m\=...{If.4..m{.X.D.C..z.b.]..r~.V...}....g..QL...|..GL|...0....l...E...u.c2..S.R.....7.f..5..;2...&Z..:.f.(Ys.X.6@.....z....J..0.Z.Y0(?.X...,.....I8.....E....
!.$..c....>.f`*4K.dM[K.hX.....$4..T....:5p..4v(d.I%.N3P.f..."......?...sC.....], .R.k.'6..;.....$;N."5eR..U9cB.k.ny....$Q..'.....ilOf.....&...RT...0y.A.[..XY.v.....^..Ru4..ow...d.k....c.~...-
..5..O5:rky.V...6...I..[3.._..W..-io.....I.V.a.@..D.....6&.6..mh[So..G.O.dO...n.....T.zBj..b.P...jS..oz..So..I..h[}..-.....".#.{.}..o2....Cn.h..E.....,X...c..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\agrandoimg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	44095
Entropy (8bit):	7.803138426094616
Encrypted:	false
SSDEEP:	768:GM0pZfXWGuvhx54uV9JdwyZjpK/CUyWTPryYQ8YvFAQqivDrfDlEaU2k:8ben4UUopihPryYQ8ejvDqaUV
MD5:	CE3ADD779A015CC98DBFDF63105778FA
SHA1:	4620EC2734A0D143D3DE384D264E74CFB7FC1CBC
SHA-256:	DDA0353609918EA926F3F5AAB60D911B59147933EFFC197D33325581AF66639B
SHA-512:	2C20751E8B2469BA7F19A7BFE518305FED565376A06C91A413636034A2B2EE325999E39B23E24A515476751EBCC1EA9E5F4578DB77B32E5B1D112E13E3F8D87F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/agrandoimg.png
Preview:	

.PNG.....IHDR... ... .p.h....sRGB.....pHYs.....+.... .IDATx....\ib...qy.gVfy..k..3..f..q.....R6V!mHW.;.....A.Z}..ZI.(j.f.Crf.g..{.a..|Uf..<N.....B.xQ.<....(w2..:.9...$l.....O.....
<?..... .....!@.....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c.....
.....!@.....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c..... .....!@.....
C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c..... .....!@.....C.....0.....
.`.....1.....c..... .....!@.....C.....0.....`.....1....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\agrandotxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	20994
Entropy (8bit):	7.462390274618951
Encrypted:	false
SSDEEP:	384:nXC6Jchvf5U6A610rBJWcZTCF6ysMVaBAY5+pEoNgl5vUOgfrXiNxk:nXCRhXy6H0LL+5a9WnSluOgfrsW
MD5:	817046BAE0190A7F0CDFE3A032ABE069
SHA1:	758108A0E8A082BA6BCEF6E0D69041E8B8431101
SHA-256:	6BDF6A507833E1B784B929E2B5CE6DF982400C6DE2AD97AE729BA3FC9D48DE84
SHA-512:	6EC5F75610361129D368D2B3D6258EC143BAE788257F77FA43CF42FDAB885807F88AA08FA1E2B16E04EAD232112AC0C2D6248064053C5EC3CBE652B64042D10
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/agrandotxt.png
Preview:	

.PNG.....IHDR... ... .p.h....sRGB.....pHYs.....+.... .IDATx...yxNw.....X. ....%.$...N...}.RcT..X..j;.N1..2.J[U.V-JK..J...Q. ....*...G.\.{9..|H=..u_W...g9'.....cSJ).....:.
.....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....
!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....
.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....
@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\al2o9zrvru7aqj8e1x2rzsrca[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 4 icons, 16x16, 32 bits/pixel, 24x24, 32 bits/pixel
Category:	downloaded
Size (bytes):	24838
Entropy (8bit):	2.3776312389302885
Encrypted:	false
SSDEEP:	96:h2ki0ihoer+JHZyx51Zc3juid220pvVhrBpvN:h2bEHK1ZxY220b
MD5:	B2CCD167C908A44E1DD69DF79382286A
SHA1:	D9349F1BDCF3C1556CD77AE1F0029475596342AA
SHA-256:	19B079C09197FBA68D021FA3BA394EC91703909FFD237EFA3EB9A2BCA13148EC
SHA-512:	A95FEB4454F74D54157E69D1491836655F2FEE7991F0F258587E80014F11E2898D466A6D57A574F59F6E155872218829A1A3DC1AD5F078B486E594E08F5A6F8D
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://static-exp1.licdn.com/sc/h/al2o9zrvru7aqj8e1x2rzsrca

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\al2o9zrvru7aqj8e1x2rzsrca[1].ico	
Preview:	..... .h...F..... ....6...@@.... .(B.....(..... ....s...s...s...s...s...s...s...s...s...s...s...s...s.../.....s...s.. .s...s...s...s...s...s...s...s...s...s...s...s.....s...s.....s...s...s.....s...s.....s...s.....s.....s...s...s.....s...s.....s...s.....s...s...s.....s...s.. .....s...s.....s.....s...y.....s...s.....s...s.....s.....z..s...D.....s...s.....s...s.....s.....s...s.....s...s.....s.....?..s...s .....s...s...=..=..s...s...s...w...~...s...s...s...s.....s...=.....=..s...s...s...s...s...s...s...s.....s...=.....=..s...s...s...s...s...s...s...s.....s...s...=..=..s...s...s...s...s.. .s...s...s...s...s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\alanimg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	16493
Entropy (8bit):	7.265809014153406
Encrypted:	false
SSDEEP:	192:ri4ykJjQ9uzqh3/Z8K72mA3bXJct7wNXZOwc2hJ2Vbl6rJrKTRBIZ:p7QYzqhJt7oZRc2hJ2Vbl6ZABk
MD5:	A2E89680040001CFB69090411D6E1890
SHA1:	DC719622CFD547BDD9470EF22375E059079AF0DD
SHA-256:	CA0B2B6E9DF72994E15437B1D9AEBCA2DB23B7F615C9D27975CFBA34B77D2DE0
SHA-512:	A58552CE33AD8AD83B82D9A45405FD0978529976F145B0CCA3A13D89CFC8A804D92B57FE4F7F9A54F7BEE1444570560727620A603F7D5771B38BAD4C12F58A8A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/alanimg.png
Preview:	.PNG.....IHDR... ... .p.h....sRGB.....pHYs.....+.... .IDATx...s..a....Z..Z.'H $...m....;@..nR'm3.L..L.....L...S;.I.M&..:$.c.....0.d..BBBB.^].+.....1.....~v9.y.....D"..... ..`]..... @.....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c..... ..... !@.....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c..... .....!@ .....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c..... .....!@.....C.....0 .....`.....1.....c..... .....!@.....C.....0.....`.....1.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\alantxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	14654
Entropy (8bit):	7.368356600280061
Encrypted:	false
SSDEEP:	192:SLbeZmzKQHrrBnYubJ8NVwIbTnH50ZqRemn0Om7Qoz2SmMtVQrK0cAUB6G8IZ:kOyryRVwsrZp3n0Ouz2SlGrK0cNsG8k
MD5:	2971D127A327F3A5024D85DD9638681C
SHA1:	B0BFA47D212981DDB9284F7840EE850247BEF73F
SHA-256:	3E7074E88A50D313EA31A3556BD5B2FE0DDCBC392E85380E54FE83C35878A9C5
SHA-512:	277EE7DDC93AF16B3E1CBDF47532C19B29C4EF7A26D407FB811914EC609AC9D6A7322E896CCED7A5741C4CA7B71A2B89C25C2E45AD6177C1CCBAB1DF63EBD7F
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/alantxt.png
Preview:	.PNG.....IHDR... ... .p.h....sRGB.....pHYs.....+.... .IDATx...{.UU.....o.....A.... .. M.Fa.....3..v...f.Y>QQy..)xM.".>HQ.T.....W...k....q.`.....k.].eY.....v.....HF ....$#@...d..... ..@2....HF..... .....$#@...d..... ..@2....HF..... .....$#@...d..... ..@2....HF..... .....$#@...d..... ..@2....HF..... .....$#@...d..... ..@2....HF..... .....$#@...d..... ..@2....HF..... .....$#@...d..... ..@2....HF..... ..... $#@...d..... ..@2....HF..... .....$#@...d..... ..@2....HF..... .....$#@...d..... ..@2....HF..... .....$#@...d..... ..@2....HF ....$#@...d..... ..@2....HF..... .....$#@...d..... ..@2....HF..... .....$#@...d..... ..@2....HF..... .....$#@...d....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\anchor[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	13276
Entropy (8bit):	5.962435914254506
Encrypted:	false
SSDEEP:	384:3/S0CoRft4h3o76+WixKS3YO7Jm9Lvq4+duiV:3/S/sftd76+twFPCZP
MD5:	A6EFBA9C755BBC5EEAF1C0DE4BDDF565
SHA1:	481AFFBE2B7FF48860246EA4E784D4557B277399
SHA-256:	E8315919B0683827E65A3AD9D566970268F24B508FA102FB9ABF7F88E6C4C77D
SHA-512:	0DFAA39D8BE8A68CEAADFF64F0E4A0493A7BAAAF976AE9C1EC13F6BC428529CF3E11EB5C6079680F75CF5048F73A017A313F8C7FC72981C554515EF4BC1DA48B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\anchor[1].htm	
Preview:	<!DOCTYPE HTML><html dir="ltr" lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.<meta http-equiv="X-UA-Compatible" content="IE=edge">.<style type="text/css">.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 400;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxP.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 500;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc9.ttf) format('truetype');.}.@font-face {. font-family: 'Roboto';. font-style: normal;. font-weight: 900;. src: url(//fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc9.ttf) format('truetype');.}..</style>.<link rel="stylesheet" type="text/css" href="https://www.gstatic.com/recaptcha/releases/jxFQ7RQ9s9HTGKeWcoa6UQdD/styles__ltr.css" nonce="GK0AcyMWHAbHdc5h/BeZ/w">.<script nonce="GK0AcyMWHAbHdc5h/BeZ/w" type="text/javascript">window['__recaptcha_api'] = 'https://www.google.c

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\apple-icon-57x57[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 57 x 57, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	1721
Entropy (8bit):	7.4411148557423115
Encrypted:	false
SSDEEP:	48:cnEjKEdg6lFC+4aCoNhzc2pMEC87D4FNAnLVlBItvjc:ayxYroNdq87kUxItvA
MD5:	1EF17839D9436C7CFF6F7F028B5CEA14
SHA1:	4882D78AADAD35304FFAF3A23F812762F151FC89
SHA-256:	B29FEF183DFF556A446157EF9C6C43AA1D241EE0FEC8DF5BC7EDE42DC280AF08
SHA-512:	D20EE7A29BA58E2009BC265CBC3928F2F51C1F4D088F7097F267C430D76237226AD5199AB2C9A3784090E28664A45162B41289D3CD1194F1A899EB6A6374D823
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/apple-icon-57x57.png
Preview:	.PNG.....IHDR...9...9.....s.....gAMA.....a.....sRGB..... cHRM..z&.....u0...`.:....p..Q<...[PLTE.....`ihr.....y..|.....EGF\ed...t..SXX.....LOO.....V\[x.....jut.....q.~.....t.....r.....GHH^fe...z..cnl.....jvublk...s..lyx.....nzy.....lxvmzyz..w..ILL.....{.....n{zp}|...s.....aji...jvt...htseon.....OTS`ji.....o}|=<<.....v.....|..dnmkwv...gsq...ius...o}{q.~...q.}>=={.....~.....JLLLPO.....KNNNRQ...{.....}.....w.....ORR...FGG]ed.....bKGD...W.....pHYs...H...H.F.k>....IDATH.c`...`...Q...Ldjdfaec`G.....W#.'.7./..#.. ...0.....8../...4#..r....+(*)s....khji.....1.....E.....K.....?@.w.0i.....u..GDFE....'x$..&%.....r,.G.sfV.H.hv.snT^.kAa.{qXli.Qy.h.../.VVU....u*x'..5X565k.....tXuv1.u.`..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\awsimg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	147141
Entropy (8bit):	7.984711773830467
Encrypted:	false
SSDEEP:	3072:oztbHOFt3adZku1Wb52GIYMYnIB2GJP1oUhJ2yEpA1fp9:oztbqQnkuy61P1oUhJlE21f
MD5:	D8BA77282C27578DD23FD263D297CA7D
SHA1:	B995D64FE73C68468C4940A8663D5D7300F0F7F8
SHA-256:	B9EBE6CA6BFCCF76C4A3C46F12B1100F036C3A5AAC07279A27FBBB80D0934FAB
SHA-512:	70738B1D85329FE2CF836F920E1A8F4682AD9D4BDB40740378B80C9A3AE4A8DD7E528579F8D3E74F13A8375979366684B5F007FA5A154F383B097D8715A16DEC
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/awsimg.png
Preview:	.PNG.....IHDR... ... .p.h....sRGB.....pHYs.....+.... .IDATx....{..}.....g..\Dj....<..]O...'".%[..S.N.$v`.Y.....@R.....IR.0....WU&.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....t.....3.....!.....@g. ....:C.....@....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\awstxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	26830
Entropy (8bit):	7.59237571530276
Encrypted:	false
SSDEEP:	768:pfffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffX:bCKJMgt+CrnamC32X
MD5:	6106CCF77B13ED96F66D31BD7CF6FE07
SHA1:	DF723B3C8D0BCCE98B5602E43410A2D86D1D1C5A
SHA-256:	BCBEF90D0BB429C453FB92512A9B2A1ECE1A794B79AC2321EAB376137F31D18D
SHA-512:	8B1BAABF491C3C931BB75BA61F044EC4DD4D96012B745CBD8C2B021130EAB20981D9D622DF17BE53DD34BCC7CA4782C4B76C3B980031C1DE333357197E3FCD2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/awstxt.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\awstxt[1].png	
Preview:	.PNG.....IHDR... ... .p.h....sRGB.....pHYs.....+.... .IDATx...g|.....P...!!t...w....P..._A..D.P<.9.(....XP.P. %..A..iJ.....O.kvg7.....17.2W..Yv.3...RJ.....c. .. ...!.....0.....c. .....!.....0.....c. .....!.....0.....c. .....!.....0.....c. .....!.....0.....c. .....!.....0.....c. .....!.....0.....c. .....!.....0..... .....c. .....!.....0.....c. .....!.....0.....c. .....!.....0.....c. .....!.....0.....c. .....!.....0.....c. .....!.....0.....c. .....!.....0.....c. .....!... ..0.....c. .....!.....0.....c. .....!.....0.....c. .....!.....0.....c. .....!.....0.....c. .....!.....0.....c. .....!.....0.....c. .....!.....0.....c. .....!.....0.....c. .....!.....0.....c. .....!.....0..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\blendimg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	23245
Entropy (8bit):	7.6164264646147375
Encrypted:	false
SSDEEP:	384:VqfSvYvQuOPUaiz5uczApeL1YijYo3UPzD6m8oCe5Pb212tvfqzJJJJJJJJJJJZ:bvuQuOJiFopeL1YijXMaboBPb2Itvfql
MD5:	7B63B0FD20DDBA6FBF7A996523A34597
SHA1:	2F672D0BC9451623DBCE7ED6BCC4D8582AB34A67
SHA-256:	39EF81F60134D396E50A8DD127D9EEDDD93C71B68157CE3E925DC7F3125296E0
SHA-512:	A9099BA5D7C157589C10E1BBE31059CDFFF7BC30AF1A5CC07BBDC1E75B4189EA25200F36206C1AC360927986636A0D48D4A24B736518B54464B15B0BE448EE5 C
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/blendimg.png
Preview:	.PNG.....IHDR... ... .p.h....sRGB.....pHYs.....+.... .IDATx...gx\.a...T..;A...l"%R..DuKr.....v.N6q...x.nv..M....nKV.%.P.).....(D.m...9..RZ...1.. ..u.u..`.=.)6.,.....>..... .....1.....c..... .....!@.....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1. .....c..... .....!@.....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c..... .....!@.....C.....0.....`.....1.....c..... .....!@.. ...C.....0.....`.....1.....c..... .....!@.....C.....0.....`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\blendtxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	19387
Entropy (8bit):	7.389053165694573
Encrypted:	false
SSDEEP:	384:iorwNNFTFR12wKhlTJj+Af4siq2h00rVNJk:ioeNBIzTJj+Qhiq2hDrVNO
MD5:	BE351FDC5E983800D71A5C0234D28C1A
SHA1:	3C27004850CC0148419D4130DF85E302B725A6B0
SHA-256:	BFAA1A2D6381C3A65488FDBADE8D40685B4C428EAD5080C1A40978AEF69C625E
SHA-512:	0E46535B5BEC3935B679BE019CB337B1FF6B4E6A8EF0E67FAD4ED6E080DE10B2DC99D92E38CBB24D278B42599E59C4E810C9075718646F888F4DFD54DD50F5/ 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/blendtxt.png
Preview:	.PNG.....IHDR... ... .p.h....sRGB.....pHYs.....+.... .IDATx...yXU..../ .....S9...).....Yf.p5....C.M.z...W..,...!...!..5G.HADq..dZ.?..#.}F.....y.....s.&....M).....4p/..... ....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!..... .@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.... ...m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@.....m. .....!.....@....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bouleimg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	33355
Entropy (8bit):	7.766262694756886
Encrypted:	false
SSDEEP:	768:tfffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffM:LwOMEOXnsaFH
MD5:	A49A509488FB5749F4C665C0D152D7E5
SHA1:	B0B8E3446829DC702506181D19896442556B6FE6
SHA-256:	513AFCD336001FB5DB0216A0CBDFF000E3C511BFB1918512FCC26F8C11DF5C46
SHA-512:	AFF84141CA6DAB794B17D2E11CADE9F46836EE28B08EC2AE3AFF446CCAD2B82C530181974494917241EE6E68F85DD01BFA1BE0BF01DE70D820882E86B4CBB1 06
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/bouleimg.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bouleimg[1].png	
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx....\......g.....DR.%R.......1.1............z,v.$R....U.j..=o../nV....@..U..'..$A...D.}...s.<.s......../....................c. .....! .....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0............. ...c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0 ....c. ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\bouletxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	16641
Entropy (8bit):	7.484577442988441
Encrypted:	false
SSDEEP:	384:KojnVd5uQ3MhNrkOPkKYFq5fJdBAIDRbk:KoXEQchNrNRf6ERI
MD5:	F7C88391A70D2F37C8BF55D1CB0A4784
SHA1:	71A1C2061B255D8430AD9DD91A2A82E937B4FD5C
SHA-256:	2CF151F33F0DA4AEA4F907C436CCD4951D4A1942ADB00DCDF2124DC96CDBA83D
SHA-512:	92F9CB29A3C4CE57CE447A792C5FF0762AA0323A4B556702906C3C35175BA7FD8EF067A3991DB546FECF82E4E7AF4D6C1194B6A6963F2BA11B4E011288DF0EC E
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/bouletxt.png
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx...{..s....ju....9.AR.4-..I..3SN..go...l...`.....1..S..PH...II..V).Zj].?f..k..O...x.?.s_...Z.Z.^..u_EY.e....@.m}.....C...... ... .$#@...d............ ..@2....HF......... .....$#@...d............ ..@2....HF......... .....$#@...d............ ..@2....HF......... .....$#@...d............ ..@2....HF......... .....$#@...d............ . .@2....HF......... .....$#@...d............ ..@2....HF......... .....$#@...d............ ..@2....HF......... .....$#@...d............ ..@2....HF......... .....$#@...d............ ..@2....HF......... .....$#@... d............ ..@2....HF......... .....$#@...d............ ..@2....HF......... .....$#@...d............ ..@2....HF......... .....$#@...d............ ..@2....HF......... .....$#@...d............ ..@2....HF......... .....$#@...d............ ..@2....HF......... .....$#@...d............ ..@2....HF......... .....$#@...d............ ..@2....HF......... .....$#@...d..........

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\burrowimg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	26587
Entropy (8bit):	7.619615139426183
Encrypted:	false
SSDEEP:	768:qlLZUZpHwWOewp/pnoi3lAkZF+9xpyBiW:WUvQWOewl1p3lBebOiW
MD5:	77068496BB8D9992D43D3EAFD520A127
SHA1:	6D57A2D5DA2C3037DD177F3962614E0CA75B7515
SHA-256:	68F7B954E4E467FE8FF042F6FBAD6984D8EB8FA39265F2F83A7C4944584759D8
SHA-512:	767BBFA5F9B6C38644A6D3BC750228CC46DD5DF0DA30933B306DA9300485E4EAD9D44CB4A2CD4C578B4BAE170912D741AAB8830A59BC9E35287BEFD7376357 7
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/burrowimg.png
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx...Yw.W....... Hp..Q.-..v:k..Z....8U98.y.8. .y..p...e...(jK>......". @.'.~.7..a(....0..........A.....`.......1........@..... C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1.. ......@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.... .`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1....... .@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.......1........@.....C.....`.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\burrowtxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	18754
Entropy (8bit):	7.353030363380436
Encrypted:	false
SSDEEP:	384:mhJy9a+qqT1RuNZywWj9almV4hKHHO/i4+X0sQBk:AJy9Vqg2P/lmV4hKO/T+EsQm
MD5:	5E1A3D504A6AC21ECE2E4A1888F83037
SHA1:	0C365D67D23CC27CA9DE97E58D6AFF5B075ACFE2
SHA-256:	069BBBEEA55F20846EC5DAE6E0773EEDD39843CC06C234C62110D1389A1E5DC8
SHA-512:	37213A24202A59BC44338F4D5951CDE7F3A50A166FFB2D49CC2E5EE4F116B1EDB78254DFB5BB08FFB9A426EAAEC11443695349DF4D91D96F1CF4CF81C6F1EF 8
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/burrowtxt.png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\burrowtxt[1].png	
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx...y\.U....;.(.*$...Y........ce.-..9j..M6S..}.6..q4.*.0Q.=.\.,.%$\.AS.e?.?._......z>.<...........R......8W.......q.@....hC. ....6........@....hC............6........@....hC............6........@....hC............6........@....hC............6........@....hC............6........@....hC............6........@....hC............6.... ....@....hC............6........@....hC............6........@....hC............6........@....hC............6........@....hC............6........@....hC............6........@....hC............6........@....hC...... ....6........@....hC............6........@....hC............6........@....hC............6........@....hC............6........@....hC............6........@....hC............6........@....hC............6........@ ....hC............6........@....hC............6........@....hC............6........@....hC............6........@....hC.........

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\carrotlogo[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	37049
Entropy (8bit):	7.80853434046181
Encrypted:	false
SSDEEP:	768:Vyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyu6zk8NPmHmHBCr/XBiIasDi/g:Wuk8hmmH8/B3aswGvbG4j
MD5:	6B6DE4C9E133CE8A90FA305AE300A50E
SHA1:	3062FC336D097CEB51651407203BBC979DC7FCC0
SHA-256:	C838733CE708F5AE398BF2B7404A469D4B19DE870AE3AA05A9A06B32D7F406D7
SHA-512:	19A51CF725A435149ADFFF2B83F356B81E96C701A1433937D9E88E0DD76F83694B7CDD43FDACE2B80E7D7627ABEB6D6E313BD01E09C53946417FBE91439D18E 0
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/carrotlogo.png
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx....s.w..../....$H....n...v..c=31.1.g..aG...}....~l...#..px&vz=3..nu.[}.$EI......*..........&...R@..:2...~..........)..z.....<:. ....RC..............@.......... 5.......!.....H......@j. ....RC..............@.......... 5.......!.....H......@j. ....RC..............@.......... 5.......!.....H......@j. ....RC..............@.......... 5.......!.... .H......@j. ....RC..............@.......... 5.......!.....H......@j. ....RC..............@.......... 5.......!.....H......@j. ....RC..............@.......... 5.......!.....H......@j. ....RC..............@.......... 5.......!.....H......@j. ....RC..............@.......... 5.......!.....H......@j. ....RC..............@.......... 5.......!.....H......@j. ....RC..............@.......... 5.......!.....H......@j. ....RC..............@... .... 5.......!.....H......@j. ....RC..............@.......... 5.......!.....H......@j. ....RC............

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\carrottxt[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	27258
Entropy (8bit):	7.588420453713797
Encrypted:	false
SSDEEP:	768:Bfffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffi:UbVI++DJ3K3yzdUHh8aj
MD5:	28CA1E80EF61B0A3CF3EBDF76EEEAC51
SHA1:	53D475CE2D9F72FBEBB01F0CCE52BF5783BA9419
SHA-256:	E2ED6DF1879A8CA07528BF9623AA361ABAD9802281ACD1A9AE71A6DEB0B214F9
SHA-512:	168A6AB8DB1FC74AF80ACDFA3F9E25ED54461C9BC3D50355A77F46F505DBD9EB39B62F53B32D6082EDBF5142F6ED0BDFD27EB02C5E11044D1368CFC703B26 89
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/carrottxt.png
Preview:	.PNG........IHDR... ... .p.h....sRGB.........pHYs..........+.... .IDATx...wt.....w.$..F..CD.*....E@.(......XP.." `.x.)..{.D.w.E.). .....%@z...........f.!...9.3;.2..d^S>.R......x......... .....0.. ....c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. ... ..!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0......... .....c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.....0.............c. .....!.... .0.............c. .....!.....0.............

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\clutterimg[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 800 x 800, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	18910
Entropy (8bit):	7.49109151176245
Encrypted:	false
SSDEEP:	384:eFXpWFNxVMqPW+bgL6O1turHd6qsVcuSnHVSn1gpyUk:0XkPjPbbzO1EsqsV3S0epyr
MD5:	4E9D713DDC34F582081E8290641823D0
SHA1:	C018F2CA08AC29BB877D9F64DDF74ED08E5FA9A3
SHA-256:	DC5F17F18385C61AC22F61E2B3AB31462538890870F1C7620EF3BA4A2926E905
SHA-512:	96E5DB6A02A14EAE4F2F28BD4090DDE1AA1AC55E2559E8CDD5DFB2D339A5DA999EF9C9D9E713A22343652E920BD2B546C3F137AF743B4F5B19B7D60683428E 9B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://assets.superlander.com/images/clutterimg.png

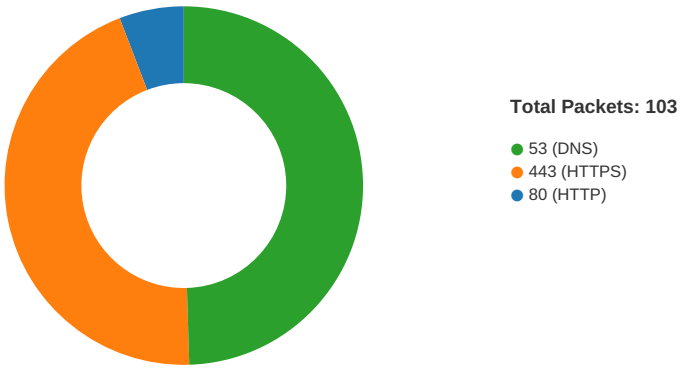
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\clutterimg[1].png	
Preview:	.PNG.....IHDR... ... .p.h....sRGB.....pHYs.....+.... .IDATx...y.N....7i63.m0....E.le+ED$QB%Z.I()Q.%.o..*D..}..3f..6fQ...[..if.s_.}..z>.=.~.9..i.....\'.k.....l;.....c(.....0

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:02:16.494018078 CET	49710	80	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:16.494225025 CET	49711	80	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:16.699965000 CET	80	49711	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:16.700007915 CET	80	49710	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:16.700108051 CET	49711	80	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:16.700158119 CET	49710	80	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:16.701152086 CET	49710	80	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:16.906874895 CET	80	49710	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:16.906903028 CET	80	49710	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:16.906996012 CET	49710	80	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:16.919287920 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.128060102 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.128257036 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.138169050 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.344345093 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.354490042 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.354532957 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.354552984 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.354634047 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.354686975 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.393625975 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.402223110 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.402466059 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.599739075 CET	443	49713	157.230.161.221	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:02:17.599766016 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.599944115 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.608210087 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.608232021 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.608876944 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.610138893 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.610193014 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.610213995 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.610234022 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.610239983 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.610269070 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.610281944 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.610305071 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.610316038 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.610342979 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.610352993 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.610378027 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.610388041 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.610424042 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.647701025 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.806520939 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.806554079 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.806574106 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.806598902 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.806694031 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.806757927 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.814810038 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:17.815520048 CET	49713	443	192.168.2.3	157.230.161.221
Feb 25, 2021 22:02:17.897486925 CET	443	49713	157.230.161.221	192.168.2.3
Feb 25, 2021 22:02:18.161545992 CET	49716	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.163921118 CET	49718	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.164697886 CET	49717	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.165268898 CET	49719	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.166784048 CET	49720	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.168545008 CET	49721	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.202445984 CET	443	49716	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.202728987 CET	49716	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.204758883 CET	443	49718	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.204862118 CET	49716	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.205020905 CET	49718	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.205449104 CET	443	49717	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.205538988 CET	49718	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.205925941 CET	443	49719	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.206350088 CET	49719	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.206492901 CET	49717	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.206883907 CET	49719	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.207758904 CET	443	49720	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.207861900 CET	49720	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.208497047 CET	49720	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.209333897 CET	443	49721	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.209471941 CET	49721	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.245615959 CET	443	49716	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.246340036 CET	443	49718	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.247468948 CET	443	49719	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.250161886 CET	443	49718	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.250183105 CET	443	49718	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.250283957 CET	49718	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.250288963 CET	443	49720	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.250634909 CET	443	49719	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.250658989 CET	443	49719	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.250763893 CET	49719	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.250910997 CET	443	49716	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.250933886 CET	443	49716	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.250988960 CET	49719	443	192.168.2.3	172.64.141.10

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:02:18.251019955 CET	49716	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.253063917 CET	443	49720	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.253086090 CET	443	49720	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.253129005 CET	49716	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.253169060 CET	49720	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.253176928 CET	49720	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.508193016 CET	49717	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.508236885 CET	49721	443	192.168.2.3	172.64.141.10
Feb 25, 2021 22:02:18.549174070 CET	443	49717	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.549200058 CET	443	49721	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.551568031 CET	443	49721	172.64.141.10	192.168.2.3
Feb 25, 2021 22:02:18.551595926 CET	443	49721	172.64.141.10	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:02:07.893901110 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:07.942652941 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:09.141655922 CET	60152	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:09.193417072 CET	53	60152	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:10.112464905 CET	57544	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:10.162728071 CET	53	57544	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:11.107903957 CET	55984	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:11.165097952 CET	53	55984	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:12.118552923 CET	64185	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:12.169902086 CET	53	64185	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:13.230345964 CET	65110	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:13.283828974 CET	53	65110	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:14.331079960 CET	58361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:14.379836082 CET	53	58361	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:15.234244108 CET	63492	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:15.293750048 CET	53	63492	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:15.479028940 CET	60831	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:15.530430079 CET	53	60831	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:16.333376884 CET	60100	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:16.483042002 CET	53	60100	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:16.540086985 CET	53195	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:16.589051008 CET	53	53195	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:17.994755030 CET	50141	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:18.012252092 CET	53023	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:18.049421072 CET	53	50141	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:18.077248096 CET	53	53023	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:18.128500938 CET	49563	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:18.182940960 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:18.184834957 CET	53	49563	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:18.210674047 CET	59349	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:18.234363079 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:18.270754099 CET	53	59349	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:18.582603931 CET	57084	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:18.631439924 CET	53	57084	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:18.679377079 CET	58823	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:18.685873032 CET	57568	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:18.728004932 CET	53	58823	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:18.737452984 CET	53	57568	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:19.175904989 CET	49563	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:19.225508928 CET	53	49563	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:19.811712980 CET	50540	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:19.854104996 CET	54366	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:19.872230053 CET	53	50540	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:19.902898073 CET	53034	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:19.908530951 CET	53	54366	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:19.965102911 CET	53	53034	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:20.171319962 CET	57762	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:20.236279964 CET	53	57762	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:02:20.484721899 CET	55435	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:20.533590078 CET	53	55435	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:20.801203012 CET	50713	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:20.854120970 CET	53	50713	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:21.423898935 CET	56132	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:21.475217104 CET	53	56132	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:21.924994946 CET	58987	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:21.976949930 CET	53	58987	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:23.027286053 CET	56579	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:23.087275982 CET	53	56579	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:24.124385118 CET	56579	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:24.181921959 CET	53	56579	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:26.245516062 CET	60633	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:26.295857906 CET	53	60633	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:27.283401012 CET	61292	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:27.334264994 CET	53	61292	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:28.207617998 CET	63619	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:28.257802963 CET	53	63619	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:35.828610897 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:35.878529072 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:39.855679989 CET	61946	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:39.919168949 CET	53	61946	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:45.145242929 CET	64910	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:45.205055952 CET	53	64910	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:45.249334097 CET	52123	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:45.301095009 CET	53	52123	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:45.940999031 CET	56130	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:45.989829063 CET	53	56130	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:46.398406982 CET	52123	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:46.450047016 CET	53	52123	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:46.952975988 CET	56130	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:47.014309883 CET	53	56130	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:47.399199009 CET	52123	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:47.453454018 CET	53	52123	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:47.968679905 CET	56130	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:48.020090103 CET	53	56130	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:49.464518070 CET	52123	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:49.518472910 CET	53	52123	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:49.970316887 CET	56130	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:50.020486116 CET	53	56130	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:50.291826963 CET	56338	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:50.352269888 CET	53	56338	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:51.495805025 CET	59420	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:51.550662041 CET	53	59420	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:53.470561028 CET	52123	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:53.522325993 CET	53	52123	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:53.739128113 CET	58784	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:53.792233944 CET	53	58784	8.8.8.8	192.168.2.3
Feb 25, 2021 22:02:53.983030081 CET	56130	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:02:54.031687975 CET	53	56130	8.8.8.8	192.168.2.3
Feb 25, 2021 22:03:03.363368034 CET	63978	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:03:03.415110111 CET	53	63978	8.8.8.8	192.168.2.3
Feb 25, 2021 22:03:09.145243883 CET	62938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 22:03:09.194272041 CET	53	62938	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 22:02:16.333376884 CET	192.168.2.3	8.8.8.8	0x5a4b	Standard query (0)	certc.com	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:17.994755030 CET	192.168.2.3	8.8.8.8	0x33c1	Standard query (0)	assets.sup erlander.com	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:18.182940960 CET	192.168.2.3	8.8.8.8	0xbde5	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 22:02:18.210674047 CET	192.168.2.3	8.8.8.8	0x6aba	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:18.679377079 CET	192.168.2.3	8.8.8.8	0x7ffa	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:18.685873032 CET	192.168.2.3	8.8.8.8	0xfc26	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:19.811712980 CET	192.168.2.3	8.8.8.8	0x6a88	Standard query (0)	d1tdp7z6w94jbb.cloudfront.net	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:19.854104996 CET	192.168.2.3	8.8.8.8	0xbe47	Standard query (0)	www.statcounter.com	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:21.423898935 CET	192.168.2.3	8.8.8.8	0x9422	Standard query (0)	c.statcounter.com	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:39.855679989 CET	192.168.2.3	8.8.8.8	0xdc3e	Standard query (0)	assets.superlander.com	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:45.145242929 CET	192.168.2.3	8.8.8.8	0x476a	Standard query (0)	statcounter.com	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:51.495805025 CET	192.168.2.3	8.8.8.8	0xee3d	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:53.739128113 CET	192.168.2.3	8.8.8.8	0x899c	Standard query (0)	static-exp1.licdn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 22:02:16.483042002 CET	8.8.8.8	192.168.2.3	0x5a4b	No error (0)	certc.com		157.230.161.221	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:18.049421072 CET	8.8.8.8	192.168.2.3	0x33c1	No error (0)	assets.superlander.com		172.64.141.10	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:18.049421072 CET	8.8.8.8	192.168.2.3	0x33c1	No error (0)	assets.superlander.com		172.64.140.10	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:18.234363079 CET	8.8.8.8	192.168.2.3	0xbde5	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 22:02:18.270754099 CET	8.8.8.8	192.168.2.3	0x6aba	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 22:02:18.728004932 CET	8.8.8.8	192.168.2.3	0x7ffa	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:18.728004932 CET	8.8.8.8	192.168.2.3	0x7ffa	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:18.737452984 CET	8.8.8.8	192.168.2.3	0xfc26	No error (0)	cdn.jsdelivr.net	dualstack.f3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 22:02:19.872230053 CET	8.8.8.8	192.168.2.3	0x6a88	No error (0)	d1tdp7z6w94jbb.cloudfront.net		13.224.94.23	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:19.872230053 CET	8.8.8.8	192.168.2.3	0x6a88	No error (0)	d1tdp7z6w94jbb.cloudfront.net		13.224.94.77	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:19.872230053 CET	8.8.8.8	192.168.2.3	0x6a88	No error (0)	d1tdp7z6w94jbb.cloudfront.net		13.224.94.88	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:19.872230053 CET	8.8.8.8	192.168.2.3	0x6a88	No error (0)	d1tdp7z6w94jbb.cloudfront.net		13.224.94.54	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:19.908530951 CET	8.8.8.8	192.168.2.3	0xbe47	No error (0)	www.statcounter.com		172.67.38.97	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:19.908530951 CET	8.8.8.8	192.168.2.3	0xbe47	No error (0)	www.statcounter.com		104.22.53.65	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:19.908530951 CET	8.8.8.8	192.168.2.3	0xbe47	No error (0)	www.statcounter.com		104.22.52.65	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:21.475217104 CET	8.8.8.8	192.168.2.3	0x9422	No error (0)	c.statcounter.com		172.67.38.97	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:21.475217104 CET	8.8.8.8	192.168.2.3	0x9422	No error (0)	c.statcounter.com		104.22.53.65	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 22:02:21.475217104 CET	8.8.8.8	192.168.2.3	0x9422	No error (0)	c.statcounter.com		104.22.52.65	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:39.919168949 CET	8.8.8.8	192.168.2.3	0xdc3e	No error (0)	assets.superlander.com		172.64.140.10	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:39.919168949 CET	8.8.8.8	192.168.2.3	0xdc3e	No error (0)	assets.superlander.com		172.64.141.10	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:45.205055952 CET	8.8.8.8	192.168.2.3	0x476a	No error (0)	statcounter.com		104.22.53.65	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:45.205055952 CET	8.8.8.8	192.168.2.3	0x476a	No error (0)	statcounter.com		104.22.52.65	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:45.205055952 CET	8.8.8.8	192.168.2.3	0x476a	No error (0)	statcounter.com		172.67.38.97	A (IP address)	IN (0x0001)
Feb 25, 2021 22:02:51.550662041 CET	8.8.8.8	192.168.2.3	0xee3d	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 22:02:53.792233944 CET	8.8.8.8	192.168.2.3	0x899c	No error (0)	static-exp1.licdn.com	2-01-2c3e-003d.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 22:02:53.792233944 CET	8.8.8.8	192.168.2.3	0x899c	No error (0)	cs1404.wpc.epsiloncdn.net		152.199.21.118	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- certc.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49710	157.230.161.221	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 22:02:16.701152086 CET	947	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: certc.com Connection: Keep-Alive
Feb 25, 2021 22:02:16.906903028 CET	952	IN	HTTP/1.1 301 Moved Permanently Server: openresty Date: Thu, 25 Feb 2021 21:13:27 GMT Content-Type: text/html Content-Length: 166 Connection: keep-alive Location: https://certc.com/ Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> openresty </body></html>

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
Feb 25, 2021 22:02:17.354552984 CET	157.230.161.221	443	192.168.2.3	49713	CN=certc.com 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.	Sat Jan 16 07:00:38 CET 2021	Fri Apr 16 08:00:38 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		
Feb 25, 2021 22:02:18.250183105 CET	172.64.141.10	443	192.168.2.3	49718	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	Thu Jul 09 02:00:00 CEST 2020	Fri Jul 09 14:00:00 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=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		
Feb 25, 2021 22:02:18.250658989 CET	172.64.141.10	443	192.168.2.3	49719	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	Thu Jul 09 02:00:00 CEST 2020	Fri Jul 09 14:00:00 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=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		
Feb 25, 2021 22:02:18.250933886 CET	172.64.141.10	443	192.168.2.3	49716	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	Thu Jul 09 02:00:00 CEST 2020	Fri Jul 09 14:00:00 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=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		
Feb 25, 2021 22:02:18.253086090 CET	172.64.141.10	443	192.168.2.3	49720	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	Thu Jul 09 02:00:00 CEST 2020	Fri Jul 09 14:00:00 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=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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 22:02:18.551595926 CET	172.64.141.10	443	192.168.2.3	49721	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	Thu Jul 09 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Jul 09 14:00:00 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		
Feb 25, 2021 22:02:18.551647902 CET	172.64.141.10	443	192.168.2.3	49717	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	Thu Jul 09 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Fri Jul 09 14:00:00 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		
Feb 25, 2021 22:02:18.911300898 CET	104.16.18.94	443	192.168.2.3	49731	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		
Feb 25, 2021 22:02:19.477010012 CET	104.16.18.94	443	192.168.2.3	49730	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		
Feb 25, 2021 22:02:19.972785950 CET	13.224.94.23	443	192.168.2.3	49734	CN=*.cloudfront.net, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Tue May 26 02:00:00 CEST 2020 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Wed Apr 21 14:00:00 CEST 2021 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 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=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		

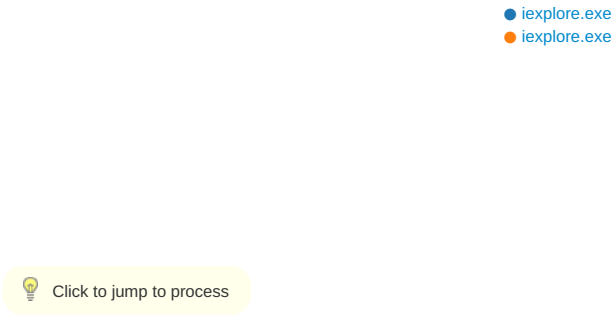
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
Feb 25, 2021 22:02:19.973946095 CET	13.224.94.23	443	192.168.2.3	49733	CN=*.cloudfront.net, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global CA G2, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Tue May 26 02:00:00 CEST 2020 Thu Aug 01 14:00:00 CEST 2013 Mon Nov 06 01:00:00 CET 2017	Wed Apr 21 14:00:00 CEST 2021 Tue Aug 01 14:00:00 CEST 2028 Sun Nov 06 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=DigiCert Global CA G2, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Aug 01 14:00:00 CEST 2013	Tue Aug 01 14:00:00 CEST 2028		
					CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US	Mon Nov 06 01:00:00 CET 2017	Sun Nov 06 00:59:59 CET 2022		
Feb 25, 2021 22:02:19.995835066 CET	172.67.38.97	443	192.168.2.3	49735	CN=us-dallas.statcounter.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 13 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Nov 14 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Feb 25, 2021 22:02:19.997082949 CET	172.67.38.97	443	192.168.2.3	49736	CN=us-dallas.statcounter.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 13 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Nov 14 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5084 Parent PID: 792

General

Start time:	22:02:13
Start date:	25/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff62ca50000
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	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

Analysis Process: iexplore.exe PID: 5188 Parent PID: 5084

General

Start time:	22:02:14
Start date:	25/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5084 CREDAT:17410 /prefetch:2
Imagebase:	0x1a0000
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	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

Disassembly